ENDPOINT ANTIVIRUS

PER MAC

Manuale dell'utente

(per la versione 6.0 e le versioni successive del prodotto)

Fare clic qui per scaricare la versione più recente di questo documento

ENDPOINT ANTIVIRUS

©ESET, spol. s.r.o.
ESET Endpoint Antivirus è stato sviluppato da ESET, spol. s r.o.
Per ulteriori informazioni, visitare il sito web www.eset.com.
Tutti i diritti riservati. Sono vietate la riproduzione, l'archiviazione in sistemi di registrazione o la trasmissione in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro della presente documentazione in assenza di autorizzazione scritta dell'autore.
ESET, spol. s r.o. si riserva il diritto di modificare qualsiasi parte dell'applicazione software descritta senza preavviso.

Supporto tecnico: www.eset.com/support

REV. 25. 8. 2015

Contenuti

1. ESET Endpoint Antivirus....4
1.1 Novità della versione 6....4
1.2 Requisiti di sistema....4
2. Utenti che si connettono tramite ESET Remote Administrator....4
2.1 Server ESET Remote Administrator....5
2.2 Console Web....5
2.3 Proxy....5
2.4 Agente....6
2.5 RD Sensor....6
3. Installazione....6
3.1 Installazione tipica....6
3.2 Installazione personalizzata....7
3.3 Installazione remota....8
3.3.1 Creazione di un pacchetto di installazione remota....8
3.3.2 Installazione remota su computer di destinazione....9
3.3.3 Disinstallazione remota....9
3.3.4 Aggiornamento remoto....9
4. Attivazione prodotto....9
5. Disinstallazione....10
6. Panoramica di base....10
6.1 Tasti di scelta rapida....10
6.2 Verifica del funzionamento del sistema....11
6.3 Cosa fare se il programma non funziona correttamente....11
7. Protezione del computer....11
7.1 Protezione antivirus e antispyware....11
7.1.1 Generale....11
7.1.1.1 Esclusioni....12
7.1.2 Protezione all'avvio....12
7.1.3 Protezione file system in tempo reale....12
7.1.3.1 Controllo al verificarsi di un evento....12
7.1.3.2 Opzioni avanzate di controllo....12
7.1.3.3 Quando modificare la configurazione della protezione in tempo reale....13
7.1.3.4 Controllo della protezione in tempo reale....13
7.1.3.5 Cosa fare se la protezione in tempo reale non funziona....13
7.1.4 Controllo del computer su richiesta....14
7.1.4.1 Tipo di controllo....14
7.1.4.1.1 Controllo intelligente....14
7.1.4.1.2 Controllo personalizzato....14
7.1.4.2 Destinazioni di controllo....15
7.1.4.3 Profili di controllo....15
7.1.5 Configurazione dei parametri del motore ThreatSense....15
7.1.5.1 Oggetti....16
7.1.5.2 Opzioni....16
7.1.5.3 Pulizia....17
7.1.5.4 Esclusioni....17
7.1.5.5 Limiti....17
7.1.5.6 Altri....17
7.1.6 Rilevamento di un'infiltrazione....18
7.2 Protezione Web e e-mail....18
7.2.1 Protezione accesso Web....18
7.2.1.1 Porte....18
7.2.1.2 Modalità attiva....19
7.2.1.3 Elenchi URL....19
7.2.2 Protezione e-mail....19
7.2.2.1 Verifica del protocollo POP3....20
7.2.2.2 Verifica del protocollo IMAP....20
7.3 Anti-Phishing....20
8. Controllo dispositivi....20
8.1 Editor regole....21
9. Strumenti....22
9.1 File di rapporto....22
9.1.1 Manutenzione rapporto....22
9.1.2 Filtraggio rapporti....23
9.2 Pianificazione attività....23
9.2.1 Creazione di nuove attività....24
9.2.2 Creazione di un'attività definita dall'utente....24
9.3 Live Grid....25
9.3.1 File sospetti....25
9.4 Quarantena....26
9.4.1 Mettere file in quarantena....26
9.4.2 Ripristino di un file in quarantena....26
9.4.3 Invio di un file dalla quarantena....26
9.5 Privilegi....26
9.6 Modalità presentazione....26
9.7 Processi in esecuzione....27
10. Interfaccia utente....28
10.1 Avvisi e notifiche....28
10.1.1 Configurazione avanzata avvisi e notifiche....28
10.2 Menu contestuale....28
11. Aggiorna....28
11.1 Configurazione dell'aggiornamento....29
11.1.1 Configurazione avanzata....29
11.2 Come creare attività di aggiornamento....30
11.3 Aggiornamento a una nuova build....30
11.4 Aggiornamenti sistema....30
12. Varie....31
12.1 Importa ed esporta impostazioni....31
12.1.1 Importa impostazioni....31
12.1.2 Esporta impostazioni....31
12.2 Configurazione del server proxy....31
12.3 Cache locale condivisa....32

1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 6 rappresenta un nuovo approccio a una protezione effettivamente integrata del computer. La versione più recente del motore di controllo ThreatSense® sfrutta la velocità e la precisione per proteggere il computer. Il risultato è un sistema intelligente che rileva continuamente attacchi e software dannosi che potrebbero minacciare il computer.

ESET Endpoint Antivirus 6 è una soluzione di protezione completa nata dall'impegno continuo basato su una combinazione tra prestazioni massime e impatto sul sistema minimo. Le tecnologie avanzate, basate sull'intelligenza artificiale, sono in grado di eliminare in modo proattivo l'infiltrazione da parte di virus, spyware, trojan horse, worm, adware, rootkit e altri attacchi Internet senza ripercussioni sulle prestazioni del sistema o interruzioni del computer.

ESET Endpoint Antivirus 6 è progettato per essere utilizzato principalmente su workstation in ambienti aziendali o commerciali di piccole dimensioni. Grazie a un utilizzo combinato con ESET Remote Administrator 6, consente di gestire facilmente qualsiasi numero di workstation client, applicare criteri e regole, monitorare i rilevamenti ed eseguire l'amministrazione remota da qualsiasi computer collegato in rete.

1.1 Novità della versione 6

L'interaccia utente grafica di ESET Endpoint Antivirus è stata completamente rinnovata allo scopo di garantire una visibilità ottimizzata e un'esperienza utente più intuitiva. Seguono alcuni dei principali miglioramenti apportati alla versione 6:

- **Protezione accesso Web**: monitora le comunicazioni tra i browser Web e i server remoti
- **Protezione e-mail**: garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP
- **Protezione Anti-Phishing**: protegge il sistema dell'utente da tentativi di acquisizione di password e altre informazioni sensibili restringendo l'accesso a siti Web dannosi camuffati da siti legittimi
- **Controllo dispositivi**: consente di controllare, bloccare o regolare le estensioni dei filtri e/o delle autorizzazioni e di definire la capacità di un utente di accedere e di utilizzare i dispositivi esterni. Questa funzione è disponibile nella versione del prodotto 6.1 e versioni successive.
- **Modalità presentazione**: consente all'utente di eseguire ESET Endpoint Antivirus in background e di disattivare le finestre popup e le attività pianificate
- **Cache locale condivisa**: consente di potenziare la velocità di controllo in ambienti virtuali

1.2 Requisiti di sistema

Per un funzionamento ottimale di ESET Endpoint Antivirus, il sistema deve soddisfare i seguenti requisiti hardware e software:

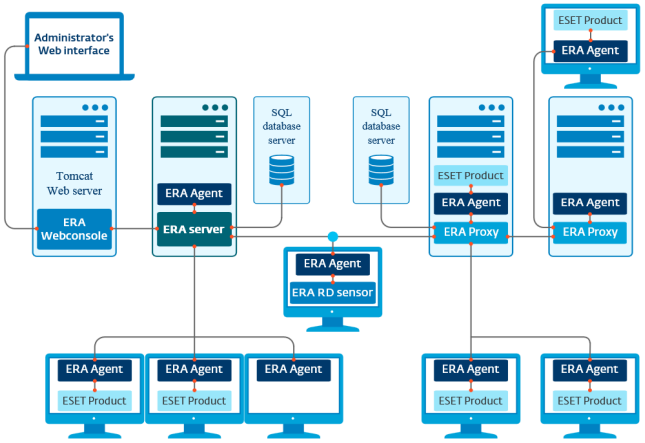
	Requisiti di sistema:
Architettura processore	Intel 32-bit, 64-bit
Sistema operativo	Mac OS X 10.6 e versioni successive Mac OS X Server 10.7 e versioni successive **NOTA:** i client che eseguono Mac OS X 10.6 non possono essere gestiti tramite ESET Remote Administrator 6.x
Memoria	300 MB
Spazio su disco	200 MB

2. Utenti che si connettono tramite ESET Remote Administrator

ESET Remote Administrator (ERA) 6 è un'applicazione che consente all'utente di gestire i prodotti ESET in un ambiente di rete da una postazione centrale. Il sistema di gestione delle attività ESET Remote Administrator consente all'utente di installare soluzioni di protezione ESET su computer remoti e di rispondere rapidamente ai nuovi problemi e alle nuove minacce. ESET Remote Administrator non offre di per sé protezione contro codici dannosi, ma si affida alla presenza di una soluzione di protezione ESET su ciascun client.

Le soluzioni di protezione ESET supportano reti che includono vari tipi di piattaforme. Una rete può integrare, ad esempio, una combinazione degli attuali sistemi operativi Microsoft, Linux e OS X e dei sistemi operativi eseguiti sui dispositivi mobili (cellulari e tablet).

L'immagine sottostante illustra un esempio di architettura per una rete protetta mediante soluzioni di protezione ESET gestite da ERA:



NOTA: per ulteriori informazioni, consultare la documentazione on-line di ESET Remote Administrator .

2.1 Server ESET Remote Administrator

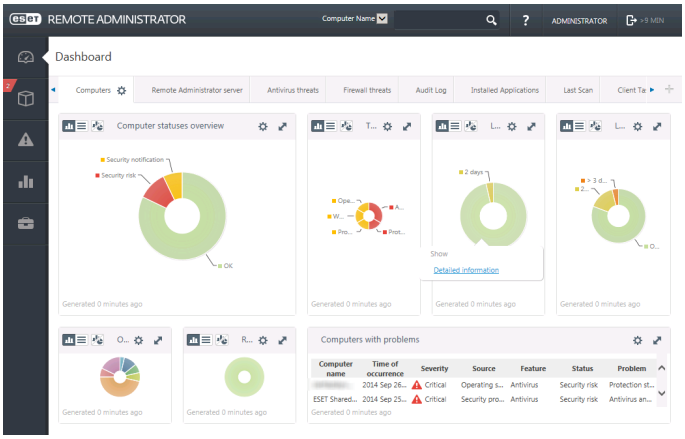
Il server ESET Remote Administrator è il componente esecutivo di ESET Remote Administrator. Elabora tutti i dati ricevuti dai client che si connettono al server (attraverso l'Agente ERA 6). L'agente ERA facilita le comunicazioni tra il client e il server. I dati (rapporti del client, configurazione, replica dell'agente, ecc.) sono archiviati in un database al quale ERA accede per fornire le segnalazioni.

Per una corretta elaborazione dei dati, il server ERA richiede una connessione stabile al server di un database. Per ottenere prestazioni ottimali, si consiglia di installare il server ERA e il database su server separati. È necessario configurare la macchina sulla quale è installato il server ERA in modo da accettare tutte le connessioni dell'agente, del proxy o di RD Sensor, che vengono verificate mediante l'utilizzo dei certificati. Dopo aver installato ERA Server, è possibile aprire ERA Web Console 5 che consente di gestire le workstation dell'endpoint su cui sono installate soluzioni ESET.

2.2 Console Web

ERA Web Console è un'interfaccia utente basata sul Web che presenta i dati provenienti dal Server ERA 5 e consente all'utente di gestire le soluzioni di protezione ESET nella rete in uso. È possibile accedere alla console Web tramite un browser. che consente di visualizzare una panoramica dello stato dei client sulla rete e di utilizzare da remoto soluzioni ESET su computer non gestiti. È possibile decidere di rendere il server Web accessibile da Internet per consentire l'utilizzo di ESET Remote Administrator praticamente da qualsiasi posizione o dispositivo.

Dashboard della console Web:



nella parte superiore della console Web, è disponibile lo strumento **Ricerca rapida**. Nel menu a discesa, selezionare **Nome computer**, **Indirizzo IPv4/IPv6** o **Nome minaccia**, digitare la stringa di ricerca nel campo di testo e fare clic sul simbolo della lente di ingrandimento oppure premere **Invio** per avviare la ricerca. L'utente verrà reindirizzato alla sezione Gruppi, dove sarà possibile visualizzare i risultati della ricerca.

2.3 Proxy

Il **Proxy ERA** è un altro componente di ESET Remote Administrator che consente di soddisfare due requisiti principali. In reti di medie dimensioni o aziendali caratterizzate dalla presenza di numerosi client (ad esempio, 10.000 client o più), è possibile utilizzare il proxy ERA per distribuire il carico tra molteplici proxy ERA, allo scopo di facilitare i compiti del Server ERA 5 principale. L'altro vantaggio del proxy ERA consiste nella possibilità di utilizzarlo per connettersi a una filiale aziendale da remoto con un collegamento debole. Ciò significa che l'agente ERA su ciascun client non si connette al server ERA principale direttamente attraverso il proxy ERA che si trova sulla stessa rete locale della filiale. Questa configurazione libera il collegamento alla filiale. Il proxy ERA accetta connessioni da tutti gli agenti ERA locali, ne compila i dati e li carica sul server ERA principale (o un altro proxy ERA). Tale operazione consente alla rete di adattare altri client senza compromettere le prestazioni della rete stessa e la qualità delle query relative al database.

In base alla configurazione della rete in uso, il proxy ERA può connettersi a un altro proxy ERA per poi connettersi al server ERA principale.

Per un corretto funzionamento del proxy ERA, il computer host sul quale è stato installato il proxy ERA deve prevedere un agente ESET installato ed essere connesso al livello superiore (l'eventuale server ERA o

un proxy ERA superiore) della rete in uso.

2.4 Agente

L'**Agente ERA** costituisce una parte essenziale del prodotto ESET Remote Administrator. Le soluzioni di protezione ESET sulle macchine client (ad esempio, ESET Endpoint Antivirus) comunicano con il server ERA attraverso l'agente. Queste comunicazioni rendono possibile la gestione delle soluzioni di protezione ESET su tutti i client remoti da una posizione centrale. L'agente raccoglie informazioni dal client e le invia al server. Se il server invia un'attività a un client, ciò significa che l'attività viene inviata all'agente che comunica quindi con il client. Tutte le comunicazioni di rete avvengono tra l'agente e la parte superiore della rete ERA, ovvero il server e il proxy.

Per connettersi al server, l'agente ESET utilizza uno dei tre metodi seguenti:

1. L'agente del client è connesso direttamente al server.
2. L'agente del client si connette mediante un proxy a sua volta connesso al server.
3. L'agente del client si connette al server mediante proxy multipli.

L'agente ESET comunica con le soluzioni ESET installate su un client, raccoglie informazioni dai programmi installati su quel client e passa le informazioni di configurazione ricevute dal server al client.

NOTA: il proxy ESET possiede il proprio agente che gestisce tutte le attività di comunicazione tra i client, altri proxy e il server.

2.5 RD Sensor

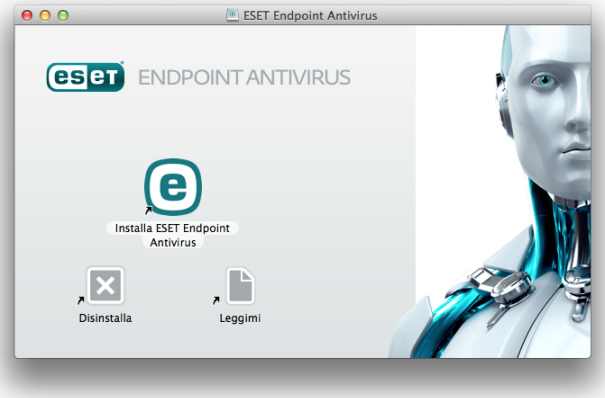
RD (Rogue Detection) Sensor è un componente di ESET Remote Administrator pensato per ricercare computer all'interno della rete in uso. È uno strumento che consente di aggiungere in modo pratico nuovi computer in ESET Remote Administrator senza che sia necessario ricercarli e aggiungerli manualmente. Ogni computer trovato nella rete viene visualizzato nella console Web e aggiunto al gruppo predefinito Tutti. Da qui, è possibile eseguire ulteriori azioni con singoli computer client.

RD Sensor è un ascoltatore passivo che rileva i computer presenti nella rete e invia le relative informazioni al server ERA. Il server ERA valuta se i PC trovati nella rete sono sconosciuti o già gestiti.

3. Installazione

Il programma di installazione di ESET Endpoint Antivirus per Mac può essere eseguito in due modi:

- Se si utilizza il CD/DVD di installazione, inserire il disco nell'unità CD/DVD-ROM e fare doppio clic sull'icona di installazione di ESET Endpoint Antivirus per lanciare il programma di installazione.
- Se si utilizza un file scaricato dal sito Web, fare doppio clic su di esso per avviare il programma di installazione.



L'installazione guidata condurrà l'utente attraverso le fasi di configurazione di base. Durante la fase iniziale dell'installazione, il programma di installazione ricercherà automaticamente l'ultima versione del prodotto on-line. Se è disponibile una versione più recente, l'utente potrà decidere di scaricarla prima di proseguire con il processo di installazione.

Dopo aver accettato i termini dell'accordo di licenza dell'utente finale, è possibile scegliere uno dei seguenti tipi di installazione:

- Installazione tipica 6
- Installazione personalizzata 7
- Installazione remota 8

3.1 Installazione tipica

La modalità installazione tipica comprende le opzioni di configurazione adatte alla maggior parte degli utenti. Queste impostazioni garantiscono livelli massimi di sicurezza, nonché prestazioni ottimali del sistema. L'installazione tipica rappresenta l'opzione predefinita consigliata nel caso in cui gli utenti non abbiano particolari necessità relative a impostazioni specifiche.

ESET Live Grid
Il Sistema di allarme immediato ESET Live Grid è uno strumento in grado di informare in modo immediato e costante ESET sulle nuove infiltrazioni allo scopo di garantire una protezione rapida ai clienti. Il sistema consente di inviare le nuove minacce al laboratorio di minacce ESET, dove vengono analizzate, elaborate e aggiunte al database delle firme antivirali. Fare clic su **Configurazione** per modificare le impostazioni dettagliate per l'invio di file sospetti. Per ulteriori informazioni, consultare Live Grid 25.

Applicazioni potenzialmente indesiderate
Il passaggio finale del processo di installazione consiste nella configurazione del rilevamento delle **Applicazioni potenzialmente indesiderate**. Tali programmi non sono necessariamente dannosi. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile notarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

Dopo aver installato ESET Endpoint Antivirus, sarà necessario eseguire un controllo del computer per ricercare eventuali codici dannosi. Nella finestra principale del programma fare clic su **Controllo computer**, quindi su **Controllo intelligente**. Per ulteriori informazioni sui controlli del computer su richiesta, si rimanda alla sezione Controllo computer su richiesta 14.

3.2 Installazione personalizzata

La modalità di installazione personalizzata è indicata per utenti esperti che desiderano modificare le impostazioni avanzate durante il processo di installazione.

Componenti di programma
ESET Endpoint Antivirus consente all'utente di installare il prodotto senza alcuni componenti principali (ad esempio, la protezione Web e e-mail). Deselezionare la casella di controllo accanto a un componente del prodotto per rimuoverlo dall'installazione.

Server proxy
In caso di utilizzo di un server proxy, è possibile definirne i parametri selezionando **Utilizzo un server proxy**. Nella finestra successiva, immettere l'indirizzo IP o URL del server proxy nel campo **Indirizzo**. Nel campo Porta, specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Se il server proxy richiede l'autenticazione, sarà necessario immettere un **Nome utente** e una **Password** validi per consentire l'accesso al server proxy. Se non si utilizza un server proxy, selezionare **Non utilizzo un server proxy**. In caso di dubbi relativi all'utilizzo di un server proxy, è possibile utilizzare le impostazioni di sistema correnti selezionando **Utilizza le impostazioni di sistema (scelta consigliata)**.

Privilegi
Nel passaggio successivo, è possibile definire gli utenti con privilegi o gruppi che saranno in grado di modificare la configurazione del programma. Dall'elenco di utenti sulla sinistra, selezionare gli utenti e **Aggiungerli** all'elenco di **Utenti con privilegi**. Per visualizzare tutti gli utenti del sistema, selezionare **Mostra tutti gli utenti**. Se l'elenco di Utenti con privilegi viene lasciato vuoto, tutti gli utenti saranno considerati utenti con privilegi.

ESET Live Grid
Il Sistema di allarme immediato ESET Live Grid è uno strumento in grado di informare in modo immediato e costante ESET sulle nuove infiltrazioni allo scopo di garantire una protezione rapida ai clienti. Il sistema consente di inviare le nuove minacce al laboratorio di minacce ESET, dove vengono analizzate, elaborate e aggiunte al database delle firme antivirali. Fare clic su **Configurazione...** per modificare le impostazioni dettagliate per l'invio di file sospetti. Per ulteriori informazioni, consultare Live Grid 25.

Applicazioni potenzialmente indesiderate
Il passaggio successivo del processo di installazione consiste nella configurazione del rilevamento delle **Applicazioni potenzialmente indesiderate**. Tali programmi non sono necessariamente dannosi. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile notarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

Dopo aver installato ESET Endpoint Antivirus, sarà necessario eseguire un controllo del computer per ricercare eventuali codici dannosi. Nella finestra principale del programma fare clic su **Controllo computer**, quindi su **Controllo intelligente**. Per ulteriori informazioni sui controlli del computer su richiesta, si rimanda a Controllo computer su richiesta 14.

3.3 Installazione remota

L'installazione remota consente di creare un pacchetto di installazione che è possibile installare su computer di destinazione utilizzando il software Remote Desktop. Al termine dell'installazione, ESET Endpoint Antivirus può essere gestito da remoto attraverso ESET Remote Administrator.

L'installazione remota avviene in due fasi:

1. Creazione di un pacchetto di installazione remota tramite il programma di installazione ESET 8
2. Installazione remota attraverso l'utilizzo del software Remote Desktop 9

L'utilizzo dell'ultima versione di ESET Remote Administrator 6, consente all'utente di eseguire anche un'installazione remota sui computer client OS X. Per istruzioni più dettagliate, seguire i passaggi descritti in questo articolo della Knowledge Base. (l'articolo potrebbe non essere disponibile nella lingua dell'utente).

3.3.1 Creazione di un pacchetto di installazione remota

Componenti di programma
ESET Endpoint Antivirus consente all'utente di installare il prodotto senza alcuni componenti principali (ad esempio, la protezione Web e e-mail). Deselezionare la casella di controllo accanto a un componente del prodotto per rimuoverlo dall'installazione.

Server proxy
In caso di utilizzo di un server proxy, è possibile definirne i parametri selezionando **Utilizzo un server proxy**. Nella finestra successiva, immettere l'indirizzo IP o URL del server proxy nel campo **Indirizzo**. Nel campo Porta, specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Se il server proxy richiede l'autenticazione, sarà necessario immettere un **Nome utente** e una **Password** validi per consentire l'accesso al server proxy. Se non si utilizza un server proxy, selezionare **Non utilizzo un server proxy**. In caso di dubbi relativi all'utilizzo di un server proxy, è possibile utilizzare le impostazioni di sistema correnti selezionando **Utilizza le impostazioni di sistema (scelta consigliata)**.

Privilegi
Nel passaggio successivo, è possibile definire gli utenti con privilegi o gruppi che saranno in grado di modificare la configurazione del programma. Dall'elenco di utenti sulla sinistra, selezionare gli utenti e **Aggiungerli** all'elenco di **Utenti con privilegi**. Per visualizzare tutti gli utenti del sistema, selezionare **Mostra tutti gli utenti**. Se l'elenco di Utenti con privilegi viene lasciato vuoto, tutti gli utenti saranno considerati utenti con privilegi.

ESET Live Grid
Il Sistema di allarme immediato ESET Live Grid è uno strumento in grado di informare in modo immediato e costante ESET sulle nuove infiltrazioni allo scopo di garantire una protezione rapida ai clienti. Il sistema consente di inviare le nuove minacce al laboratorio di minacce ESET, dove vengono analizzate, elaborate e aggiunte al database delle firme antivirali. Fare clic su **Configurazione...** per modificare le impostazioni dettagliate per l'invio di file sospetti. Per ulteriori informazioni, consultare Live Grid 25.

Applicazioni potenzialmente indesiderate
Il passaggio successivo del processo di installazione consiste nella configurazione del rilevamento delle **Applicazioni potenzialmente indesiderate**. Tali programmi non sono necessariamente dannosi. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile notarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

File di installazione remota
Nell'ultimo passaggio dell'installazione guidata, selezionare una cartella di destinazione per il pacchetto di installazione *(esets_remote_Install.pkg)*, lo shell script di configurazione *(esets_setup.sh)* e lo shell script di disinstallazione *(esets_remote_UnInstall.sh)*.

3.3.2 Installazione remota su computer di destinazione

ESET Endpoint Antivirus può essere installato sui computer di destinazione attraverso Apple Remote Desktop o qualsiasi altro strumento in grado di supportare l'installazione di pacchetti Mac standard (*.pkg*), copiando i file ed eseguendo gli script shell sui computer di destinazione.

Per installare ESET Endpoint Antivirus attraverso Apple Remote Desktop:

1. Fare clic sull'icona **Copia** in Apple Remote Desktop.
2. Fare clic su **+**, accedere allo shell script di installazione *(esets_setup.sh)* e selezionarlo.
3. Selezionare **/tmp** dal menu a discesa **Posiziona elementi in** e fare clic su **Copia**.
4. Fare clic su **Installa** per inviare il pacchetto ai computer di destinazione.

Per istruzioni più dettagliate sulle modalità di gestione dei computer client attraverso ESET Remote Administrator si rimanda alla ESET Remote Administrator documentazione online.

3.3.3 Disinstallazione remota

Per disinstallare ESET Endpoint Antivirus dai computer client:

1. Utilizzando il comando **Copia elementi** in Apple Remote Desktop, individuare lo script shell della disinstallazione (*esets_remote_unInstall.sh* creato insieme al pacchetto di installazione) e copiarlo nella directory /tmp sui computer di destinazione (ad esempio, */tmp/esets_remote_uninstall.sh*).
2. Selezionare Utente sotto a **Esegui comando come**, quindi digitare **radice** nel campo **Utente**.
3. Fare clic su **Invia**. Una volta completata la disinstallazione, verrà visualizzato un registro della console.

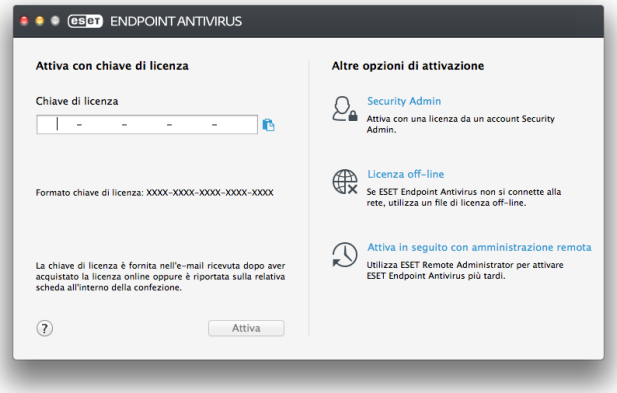
3.3.4 Aggiornamento remoto

Utilizzare il comando **Installa pacchetti** in Apple Remote Desktop per installare l'ultima versione di ESET Endpoint Antivirus in caso di disponibilità di una nuova versione.

4. Attivazione prodotto

Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto. È possibile utilizzare vari metodi di attivazione. La disponibilità di un particolare metodo di attivazione potrebbe variare in base al paese e ai mezzi di distribuzione (CD/DVD, pagina Web ESET, ecc.) per il prodotto.

Per attivare la copia di ESET Endpoint Antivirus direttamente dal programma, fare clic sull'icona ESET Endpoint Antivirus posizionata nella barra dei menu di OS X (parte superiore della schermata) e fare clic su **Attivazione prodotto**. È inoltre possibile attivare il prodotto dal menu principale sotto a **Guida** > **Attiva Licenza** o **Stato protezione** > **Attiva prodotto**.


ENDPOINT ANTIVIRUS
Attiva con chiave di licenza
Chiave di licenza
Formato chiave di licenza: XXXX-XXXX-XXXX-XXXX-XXXX
La chiave di licenza è fornita nell'e-mail ricevuta dopo aver acquistato la licenza online oppure è riportata sulla relativa scheda all'interno della confezione.
Attiva
Altre opzioni di attivazione
Security Admin
Attiva con una licenza da un account Security Admin.
Licenza off-line
Se ESET Endpoint Antivirus non si connette alla rete, utilizza un file di licenza off-line.
Attiva in seguito con amministrazione remota
Utilizza ESET Remote Administrator per attivare ESET Endpoint Antivirus più tardi.

È inoltre possibile utilizzare uno dei metodi che seguono per attivare ESET Endpoint Antivirus:

- **Attiva con chiave di licenza** - Stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della stessa. La chiave di licenza è fornita nell'e-mail ricevuta dopo aver effettuato l'acquistato oppure è riportata sulla relativa scheda all'interno della confezione.
- **Security Admin**: account creato sul portale di ESET License Administrator con le credenziali (indirizzo e-mail + password). Questo metodo consente all'utente di gestire licenze multiple da un'unica posizione.
- **Licenza off-line** - File generato automaticamente che verrà trasferito al prodotto ESET allo scopo di fornire le informazioni sulla licenza. Il file della licenza off-line viene generato dal portale di ESET License Administrator e utilizzato in ambienti in cui l'applicazione non può effettuare la connessione all'autorità che ha concesso la licenza.

Fare clic su **Attiva in seguito con RA** se il computer in uso fa parte di una rete gestita e l'amministratore prevede di utilizzare ESET Remote Administrator per attivare il prodotto. È inoltre possibile utilizzare questa opzione se si desidera attivare il client in un momento successivo.

NOTA: ESET Remote Administrator è in grado di attivare i computer client in modo silenzioso attraverso l'utilizzo delle licenze messe a disposizione dell'amministratore.

5. Disinstallazione

Il programma di disinstallazione di ESET Endpoint Antivirus per Mac può essere eseguito in più modi:

- inserire il CD/DVD di installazione di ESET Endpoint Antivirus nel computer, aprirlo dal desktop o dalla finestra del **Finder** e fare doppio clic su **Disinstalla**
- aprire il file di installazione di ESET Endpoint Antivirus (*.dmg*) e fare doppio clic su **Disinstalla**
- lanciare il **Finder**, aprire la cartella **Applicazioni** sul disco rigido, premere CTRL, fare clic sull'icona di **ESET Endpoint Antivirus** e selezionare **Mostra contenuti pacchetto**. Aprire la cartella **Contents**Risorse**Helpers** e fare doppio clic sull'icona **Uninstaller**.

6. Panoramica di base

La finestra principale di ESET Endpoint Antivirus è suddivisa in due sezioni principali. La finestra primaria sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Le seguenti sezioni sono accessibili dal menu principale:

- **Stato protezione** - fornisce informazioni relative allo stato di protezione del computer, del Web e delle e-mail.
- **Controllo computer** - questa sezione consente di configurare e avviare il Controllo del computer su richiesta 14.
- **Aggiorna** - consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.
- **Configurazione**: selezionare questa sezione per regolare il livello di protezione del computer.
- **Strumenti** - consente di accedere ai File di rapporto 22, alla Pianificazione attività 23, alla Quarantena 26, ai Processi in esecuzione 27 e ad altre funzionalità del programma.
- **Guida** - consente di visualizzare l'accesso ai file della guida, alla Knowledge base su Internet, al modulo di richiesta di assistenza al Supporto tecnico e ad altre informazioni sul programma.

6.1 Tasti di scelta rapida

I tasti di scelta rapida che è possibile utilizzare con ESET Endpoint Antivirus sono:

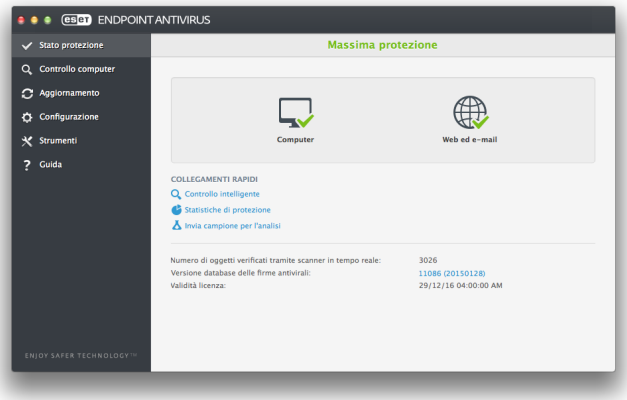
- *cmd+,*: consente di visualizzare le preferenze di ESET Endpoint Antivirus,
- *cmd+O*; consente di ripristinare le dimensioni predefinite della finestra principale dell'interfaccia utente grafica di ESET Endpoint Antivirus e di spostarla al centro della schermata,
- *cmd+Q*: nasconde la finestra principale dell'interfaccia utente grafica di ESET Endpoint Antivirus. Per aprirla, fare clic sull'icona di ESET Endpoint Antivirus nella barra dei menu di OS X (parte superiore della schermata),
- *cmd+W*: chiude la finestra principale dell'interfaccia utente grafica di ESET Endpoint Antivirus.

I seguenti tasti di scelta rapida funzionano solo se viene attivato **Utilizza menu standard** sotto a **Configurazione** > **Inserisci preferenze applicazione...** > **Interfaccia**:

- *cmd+alt+L* - apre la sezione **File di rapporto**,
- *cmd+alt+S* - apre la sezione **Pianificazione attività**,
- *cmd+alt+Q* - apre la sezione **Quarantena**.

6.2 Verifica del funzionamento del sistema

Per visualizzare lo stato di protezione, fare clic su **Stato protezione** nel menu principale. Nella finestra principale verrà visualizzato un rapporto di funzionamento dei moduli di ESET Endpoint Antivirus.



6.3 Cosa fare se il programma non funziona correttamente

Se un modulo funziona correttamente, verrà visualizzata un'icona di controllo verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione. Nella finestra principale del programma verranno visualizzate ulteriori informazioni sul modulo e una soluzione consigliata del problema. Per modificare lo stato di ciascun modulo, fare clic sul collegamento blu sotto a ciascun messaggio di notifica.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, è possibile condurre una ricerca nella Knowledge Base ESET oppure contattare il Supporto tecnico ESET che. risponderà prontamente alle domande degli utenti fornendo assistenza nella risoluzione di qualsiasi problema con ESET Endpoint Antivirus.

7. Protezione del computer

È possibile trovare la configurazione del computer sotto a **Configurazione** > **Computer**, in cui. viene visualizzato lo stato della **Protezione file system in tempo reale**. Per disattivare i singoli moduli, impostare il modulo desiderato sullo stato **DISATTIVATO**. Tenere presente che in questo modo si potrebbe ridurre il livello di protezione del computer. Per accedere alle impostazioni dettagliate di ciascun modulo, fare clic su **Configurazione**.

7.1 Protezione antivirus e antispyware

La protezione antivirus difende il sistema da attacchi dannosi, modificando i file che rappresentano minacce potenziali. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla bloccandola e pulendola, eliminandola o mettendola in quarantena.

7.1.1 Generale

Nella sezione **Generale** (**Configurazione** > **Inserisci preferenze applicazione...** > **Generale**), è possibile attivare il rilevamento dei seguenti tipi di applicazioni:

- **Applicazioni potenzialmente indesiderate** - Si tratta di applicazioni non necessariamente dannose. Tuttavia, esse potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. I cambiamenti più significativi comprendono finestre popup indesiderate, attivazione ed esecuzione di processi nascosti, aumento dell'utilizzo delle risorse di sistema, modifiche dei risultati delle ricerche e applicazioni che comunicano con server remoti.
- **Applicazioni potenzialmente pericolose** - Tali applicazioni rappresentano software commerciali e legali che possono essere sfruttati dagli autori di un attacco se installati senza il consenso dell'utente. Poiché tale classificazione comprende programmi quali strumenti di accesso remoto, questa opzione è disattivata per impostazione predefinita.
- **Applicazioni sospette** - Queste applicazioni comprendono programmi compressi mediante packer o programmi di protezione. Questi tipi di programmi di protezione sono spesso sfruttati dagli autori di malware allo scopo di eludere il rilevamento. Un packer è un file eseguibile autoestraente di runtime che include vari tipi di malware all'interno di un unico pacchetto. I packer più comuni sono UPX, PE_Compact, PKLite e ASPack. Il rilevamento dello stesso malware può variare in caso di utilizzo di packer diversi. I packer sono anche in grado di far mutare nel tempo le loro "firme", rendendo più complesse le operazioni di rilevamento e di rimozione del malware.

Per configurare le Esclusioni di file system oppure di Web e e-mail 12, fare clic su **Configurazione**.

7.1.1.1 Esclusioni

Nella sezione **Esclusioni** è possibile escludere alcuni file/cartelle, applicazioni o indirizzi IP/IPv6 dal controllo.

I file e le cartelle presenti nella scheda **File System** saranno esclusi da tutti i controlli: all'avvio, in tempo reale e su richiesta (Controllo computer).

- **Percorso** - percorso dei file e delle cartelle esclusi
- **Minaccia** - se è presente il nome di una minaccia accanto a un file escluso, ciò significa che il file viene escluso solo per quella minaccia e non per tutte. Se il file si infetta successivamente con altri malware, esso verrà rilevato dal modulo antivirus.
- [+]: crea una nuova esclusione. Inserire il percorso a un oggetto (è anche possibile utilizzare i caratteri jolly *e ?) o selezionare la cartella o il file dalla struttura ad albero.
- [−]: rimuove le voci selezionate
- **Impostazioni predefinite**: annulla tutte le esclusioni

Nella scheda **Web e e-mail**, è possibile escludere alcune **Applicazioni** o alcuni **Indirizzi IP/IPv6** dal controllo del protocollo.

7.1.2 Protezione all'avvio

Il controllo dei file all'avvio effettua un controllo automatico dei file all'avvio del sistema. Per impostazione predefinita, questo controllo viene eseguito periodicamente come attività pianificata dopo l'accesso di un utente o un aggiornamento del database delle firme antivirali. Per modificare le impostazioni dei parametri del motore ThreatSense applicabili al Controllo all'avvio, fare clic su **Configurazione**. Per ulteriori informazioni sulla configurazione del motore ThreatSense, consultare questa sezione 15.

7.1.3 Protezione file system in tempo reale

La protezione file system in tempo reale controlla tutti i tipi di supporto e attiva un controllo quando si verificano determinati eventi. Mediante la tecnologia ThreatSense (descritta in Configurazione dei parametri del motore ThreatSense 15), la protezione file system in tempo reale potrebbe essere diversa per i file appena creati o quelli esistenti. È possibile controllare con maggiore precisione i nuovi file creati.

In base alle impostazioni predefinite, la protezione in tempo reale viene avviata automaticamente all'avvio del sistema e fornisce un controllo ininterrotto. In casi speciali (ad esempio, in caso di conflitto con un altro scanner in tempo reale), la protezione in tempo reale può essere interrotta facendo clic sull'icona di ESET Endpoint Antivirus collocata sulla barra dei menu (sulla parte superiore dello schermo) e selezionando **Disattiva la protezione file system in tempo reale**. La protezione file system in tempo reale può essere disattivata anche dalla finestra principale del programma (fare clic su **Configurazione** > **Computer** e impostare la **Protezione file system in tempo reale** su **DISATTIVATA**).

Per modificare le impostazioni avanzate della protezione file system in tempo reale, accedere a **Configurazione** > **Inserisci preferenze applicazione...** (oppure premere *cmd+,*) > **Protezione in tempo reale** e fare clic su **Configurazione...**accanto a **Opzioni avanzate** (descritte in Opzioni avanzate di controllo 12).

7.1.3.1 Controllo al verificarsi di un evento

Per impostazione predefinita, il controllo viene effettuato all'apertura, durante la creazione l'esecuzione dei file. Si consiglia di mantenere queste impostazioni come predefinite per garantire il massimo livello di protezione in tempo reale per il computer in uso.

7.1.3.2 Opzioni avanzate di controllo

In questa finestra è possibile definire le tipologie di oggetti da sottoporre a controllo da parte del motore ThreatSense e attivare/disattivare l'**Euristica avanzata**, nonché modificare le impostazioni degli archivi e della cache file.

Si consiglia di non modificare i valori predefiniti nella sezione **Impostazioni predefinite archivi** salvo nel caso in cui fosse necessario risolvere un problema specifico, poiché livelli di nidificazione degli archivi troppo elevati possono ostacolare le prestazioni del sistema.

È possibile passare al controllo euristica avanzata di ThreatSense per i file eseguiti, creati e modificati separatamente selezionando la casella di controllo **Euristica avanzata** nelle rispettive sezioni dei parametri di ThreatSense.

Al fine di ridurre al minimo l'impatto sul sistema durante l'utilizzo della protezione in tempo reale, è possibile definire le dimensioni della cache di ottimizzazione. La cache di ottimizzazione viene utilizzata in caso di attivazione di **Attiva pulisci cache file**. Quando questa funzione è disattivata, tutti i file vengono sottoposti a controllo a ogni accesso. I file non verranno sottoposti a controllo ripetutamente dopo essere stati memorizzati nella cache (salvo il caso in cui siano stati modificati) fino alle dimensioni definite della cache. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali.

Fare clic su **Attiva pulisci cache file** per attivare/disattivare questa funzione. Per specificare le dimensioni della cache, inserire il valore desiderato nel campo di inserimento accanto a **Dimensioni cache**.

È possibile impostare ulteriori parametri di controllo nella finestra **Configurazione motore ThreatSense**. È possibile definire il tipo di **Oggetti** da sottoporre a controllo, le **Opzioni** da utilizzare e il livello di **Pulizia** e definire le **Estensioni** e i **Limiti** delle dimensioni dei file per la protezione file system in tempo reale. È possibile accedere alla finestra di configurazione del motore ThreatSense facendo clic su **Configurazione** accanto a **Motore ThreatSense** nella finestra di Configurazione avanzata. Per ulteriori informazioni relative ai parametri del motore ThreatSense, consultare Configurazione parametri motore ThreatSense 15.

7.1.3.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Agire con prudenza nel momento in cui si modificano i parametri della protezione in tempo reale. È consigliabile modificarli solo in casi specifici, come ad esempio il caso in cui. si verifichi un conflitto con una determinata applicazione o con lo scanner in tempo reale di un altro programma antivirus.

Dopo l'installazione di ESET Endpoint Antivirus, tutte le impostazioni sono ottimizzate al fine di offrire il massimo livello di protezione del sistema agli utenti. Per ripristinare le impostazioni predefinite, fare clic sul pulsante **Impostazioni predefinite** posizionato nell'angolo in basso a sinistra della finestra **Protezione in tempo reale** (**Configurazione** > **Inserisci preferenze applicazione...** > **Protezione in tempo reale**).

7.1.3.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare il file di test eicar.com. Questo file di test è un file speciale, innocuo e rilevabile da tutti i programmi antivirus. Il file è stato creato dall'istituto EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus.

Per controllare lo stato della Protezione in tempo reale senza utilizzare ESET Remote Administrator, effettuare la connessione al computer client da remoto utilizzando il **Terminale** ed eseguire il seguente comando:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Lo stato dello scanner in tempo reale verrà visualizzato come `RTPStatus=Enabled` o `RTPStatus=Disabled`.

L'output del bash del terminale include i seguenti stati:

- la versione di ESET Endpoint Antivirus installata sul computer client
- data e versione del database delle firme antivirali
- percorso al server di aggiornamento

NOTA: l'utilizzo dell'utility Terminale è consigliato esclusivamente agli utenti avanzati.

7.1.3.5 Cosa fare se la protezione in tempo reale non funziona

Nel prossimo capitolo verranno illustrate situazioni problematiche che si possono verificare quando si utilizza la protezione in tempo reale e verranno descritte le relative modalità di risoluzione.

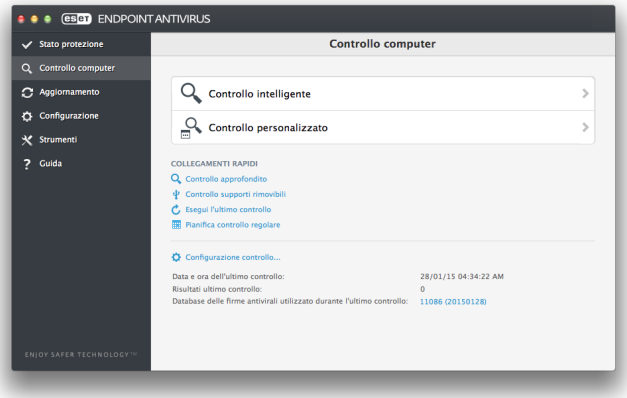
La protezione in tempo reale è disattivata
Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, dal menu principale fare clic su **Configurazione** > **Computer** e impostare la **Protezione file system in tempo reale** sullo stato **ATTIVATA**. In alternativa, è possibile attivare la protezione file system in tempo reale nella finestra Preferenze applicazione sotto a **Protezione in tempo reale** selezionando **Attiva protezione file system in tempo reale**.

La protezione in tempo reale non rileva né pulisce le infiltrazioni
Assicurarsi che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, essi possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus che potrebbero essere presenti nel sistema.

La protezione in tempo reale non viene avviata
Se la protezione in tempo reale non si attiva all'avvio del sistema, ciò potrebbe dipendere da conflitti con altri programmi. Se si dovesse verificare questo problema, contattare il Supporto tecnico ESET.

7.1.4 Controllo del computer su richiesta

Se si sospetta che il computer sia infetto perché non funziona normalmente, eseguire un **Controllo intelligente** per ricercare eventuali infiltrazioni nel computer. Per garantire un livello massimo di protezione, è necessario eseguire periodicamente controlli del computer come parte delle misure di sicurezza di routine, anziché limitarsi a eseguirli in caso di infezioni sospette. Un controllo periodico consente di rilevare infiltrazioni non rilevate dallo scanner in tempo reale se salvate su disco. Ciò accade se, al momento dell'infezione, lo scanner in tempo reale è stato disattivato o quando il database di firme antivirali è obsoleto.



È consigliabile eseguire un controllo su richiesta del computer almeno una volta al mese. Il controllo può essere configurato come attività pianificata in **Strumenti** > **Pianificazione attività**.

È inoltre possibile trascinare i file e le cartelle selezionati dal Desktop o dalla finestra del **Finder** nella schermata principale di ESET Endpoint Antivirus, sull'icona del dock, sull'icona della barra dei menu (parte superiore della schermata) o sull'icona dell'applicazione (collocata nella cartella */Applicazioni*).

7.1.4.1 Tipo di controllo

Sono disponibili due tipologie di controllo del computer su richiesta. **Controllo intelligente**, che consente di eseguire rapidamente il controllo del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato**, che consente di selezionare uno dei profili di controllo predefiniti, nonché di scegliere destinazioni di controllo specifiche.

7.1.4.1.1 Controllo intelligente

La funzione Controllo intelligente consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio principale è la semplicità della procedura, che non richiede una configurazione dettagliata del controllo. Il Controllo intelligente consente di effettuare un controllo di tutti i file presenti nelle cartelle, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulizia viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di pulizia, consultare Pulizia 17.

7.1.4.1.2 Controllo personalizzato

Il **Controllo personalizzato** consente all'utente di specificare parametri quali destinazioni e metodi di controllo. Il vantaggio del controllo personalizzato consiste nella possibilità di configurare i parametri di controllo in dettaglio. È possibile salvare diverse configurazioni come profili di controllo definiti dagli utenti. Questi sono particolarmente utili se il controllo viene eseguito più volte utilizzando gli stessi parametri.

Per scegliere le destinazioni di controllo, selezionare **Controllo computer** > **Controllo personalizzato**, quindi **Destinazioni di controllo** specifiche dalla struttura ad albero. Una destinazione di controllo può anche essere specificata in modo più preciso, immettendo il percorso alla cartella o al/i file che si desidera includere nel controllo. Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. È inoltre possibile scegliere tra tre livelli di pulizia facendo clic su **Configurazione...** > **Pulizia**.

NOTA: l'esecuzione di controlli del computer attraverso il controllo personalizzato è un'operazione raccomandata solo per gli utenti avanzati con precedenti esperienze di utilizzo di programmi antivirus.

7.1.4.2 Destinazioni di controllo

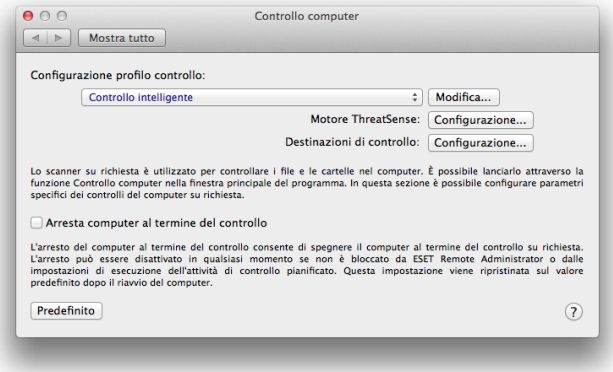
La struttura ad albero delle destinazioni di controllo consente di selezionare i file e le cartelle da sottoporre a controllo antivirus. È altresì possibile selezionare le cartelle in base alle impostazioni di un determinato profilo.

Una destinazione di controllo può essere specificata in modo più preciso, immettendo il percorso alla cartella o al/i file che si desidera includere nel controllo. Scegliere le destinazioni dalla struttura ad albero contenente un elenco di tutte le cartelle presenti nel computer selezionando la casella di controllo corrispondente a un dato file o a una data cartella.

7.1.4.3 Profili di controllo

È possibile salvare le impostazioni di controllo preferite per controlli futuri. È consigliabile creare un profilo differente (con diverse destinazioni di controllo, metodi di controllo e altri parametri) per ciascun controllo utilizzato abitualmente.

Per creare un nuovo profilo, dal menu principale fare clic su **Configurazione** > **Inserisci preferenze applicazione...** (oppure premere *cmd+,*) > **Controllo computer** e fare clic su **Modifica** accanto all'elenco dei profili correnti.


Controllo computer
Mostra tutto
Configurazione profilo controllo:
Controllo intelligente
Modifica...
Motore ThreatSense:
Configurazione...
Destinazioni di controllo:
Configurazione...
Lo scanner su richiesta è utilizzato per controllare i file e le cartelle nel computer. È possibile lanciarlo attraverso la funzione Controllo computer nella finestra principale del programma. In questa sezione è possibile configurare parametri specifici dei controlli del computer su richiesta.
Arresta computer al termine del controllo
L'arresto del computer al termine del controllo consente di spegnere il computer al termine del controllo su richiesta. L'arresto può essere disattivato in qualsiasi momento se non è bloccato da ESET Remote Administrator o dalle impostazioni di esecuzione dell'attività di controllo pianificato. Questa impostazione viene ripristinata sul valore predefinito dopo il riavvio del computer.
Predefinito
?

Per ricevere assistenza nella creazione di un profilo di controllo adatto alle proprie esigenze, si rimanda alla sezione Configurazione parametri motore ThreatSense 15 contenente una descrizione di ciascun parametro di configurazione del controllo.

Esempio: Si supponga di voler creare il proprio profilo di controllo e che la configurazione del controllo intelligente sia appropriata solo in parte, in quanto non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose, bensì si intende applicare l'opzione di Massima pulizia. Nella finestra **Elenco profili scanner su richiesta**, digitare il nome del profilo, fare clic su **Aggiungi** e confermare facendo clic su **OK**. Regolare i parametri in base alle proprie esigenze utilizzando le impostazioni del **Motore ThreatSense** e delle **Destinazioni di controllo**.

Se si desidera arrestare il sistema operativo e spegnere il computer al termine di un controllo su richiesta, utilizzare l'opzione **Arresta computer al termine del controllo**.

7.1.5 Configurazione dei parametri del motore ThreatSense

ThreatSense è una tecnologia proprietaria di ESET che comprende vari metodi complessi di rilevamento delle minacce. Questa tecnologia è proattiva, il che significa che fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. La tecnologia utilizza una combinazione di vari metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per garantire un notevole potenziamento della protezione del sistema. Il motore di controllo è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la velocità di rilevamento. La tecnologia ThreatSense è inoltre in grado di bloccare i rootkit.

Le opzioni di configurazione della tecnologia ThreatSense consentono di specificare vari parametri di controllo:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulizia e così via.

Per configurare i parametri del motore ThreatSense per i diversi moduli del prodotto, fare clic su **Configurazione > Inserisci preferenze applicazione**, quindi su **Protezione all'avvio**, **Protezione in tempo reale** o **Controllo computer**, in base al modulo per il quale si desiderano modificare le impostazioni**.** Fare clic su Configurazione accanto a Motore ThreatSense per rendere le modifiche della configurazione specifiche per il modulo del prodotto in questione. Le impostazioni della configurazione del motore ThreatSense sono suddivise in cinque schede in cui l'utente può configurare i tipi di oggetti da controllare, i metodi di controllo, le impostazioni di pulizia, le estensioni dei file da escludere, i limiti delle dimensioni dei file durante il controllo e l'utilizzo dell'Ottimizzazione intelligente. Le impostazioni contenute in ciascuna scheda sono descritte nelle seguenti sezioni. Fare clic su OK dopo aver completato le modifiche per applicare le impostazioni al modulo del prodotto selezionato.

- **Protezione all'avvio** - Controllo automatico dei file all'avvio
- **Protezione in tempo reale** - Protezione file system in tempo reale
- **Controllo computer** - Controllo del computer su richiesta.

I parametri di ThreatSense sono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica delle impostazioni per il controllo degli eseguibili compressi o per l'attivazione del controllo euristica avanzata nel modulo di protezione del file system in tempo reale potrebbe risultare in un rallentamento del sistema. È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, con l'eccezione del Controllo computer.

7.1.5.1 Oggetti

Nella sezione **Oggetti**, è possibile definire i file nei quali verranno ricercate le infiltrazioni.

- **Collegamenti simbolici** - (solo per Controllo computer): controlla i file contenenti una stringa di testo interpretata come percorso a un file o a una directory.
- **File di e-mail** - (non disponibile nella Protezione in tempo reale) controlla i file di e-mail.
- **Caselle di posta** - (non disponibile nella Protezione in tempo reale): controlla le caselle di posta dell'utente presenti nel sistema. Un uso scorretto di questa opzione potrebbe determinare un conflitto con il client di posta. Per ulteriori informazioni relative ai vantaggi e agli svantaggi di tale opzione, consultare il seguente articolo della Knowledge Base .
- **Archivi** - (non disponibile nella Protezione in tempo reale) controlla i file compressi in archivi (.rar, .zip, .arj, .tar e così via).
- **Archivi autoestraenti** - (non disponibile nella Protezione in tempo reale) controlla i file contenuti in file di archivi autoestraenti.
- **Eseguibili compressi** - diversamente dagli archivi standard, gli eseguibili compressi si decomprimono nella memoria. Selezionando questa opzione, verranno controllate anche le utilità di compressione statiche standard (ad esempio, UPX, yoda, ASPack ed FGS).

7.1.5.2 Opzioni

Nella sezione **Opzioni**, è possibile selezionare i metodi utilizzati durante un controllo del sistema. Sono disponibili le seguenti opzioni:

- **Euristica** - L'euristica utilizza un algoritmo che analizza le attività (dannose) dei programmi. Il vantaggio principale del rilevamento euristico consiste nella possibilità di rilevare un nuovo software dannoso che in precedenza non esisteva o che non era incluso nell'elenco dei virus conosciuti (database di firme antivirali).
- **Euristica avanzata** - L'euristica avanzata comprende un esclusivo algoritmo di euristica sviluppato da ESET e ottimizzato per il rilevamento di worm e trojan horse scritti in linguaggi di programmazione di alto livello. Grazie all'euristica avanzata, la capacità di rilevamento del programma è decisamente più elevata.

7.1.5.3 Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia:

- **Nessuna pulizia** - I file infetti non vengono puliti automaticamente. Il programma consentirà di visualizzare una finestra di avviso per consentire all'utente di scegliere un'azione.
- **Pulizia standard** - Il programma tenterà di pulire o di eliminare automaticamente un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma proporrà una serie di azioni di follow-up. La scelta tra queste azioni verrà visualizzata anche nel caso in cui non possa essere completata un'azione predefinita.
- **Pulizia approfondita** - Il programma pulirà o eliminerà tutti i file infetti (inclusi gli archivi). Le uniche eccezioni sono rappresentate dai file di sistema. Se non è possibile pulire un file, l'utente riceverà una notifica e gli verrà chiesto di selezionare il tipo di azione da intraprendere.

Avviso: nella modalità di pulizia standard predefinita, vengono eliminati interi file di archivio solo se tutti i file contenuti sono infetti. Se un archivio contiene file legittimi, nonché file infetti, non verrà eliminato. Se nella modalità di Massima pulizia viene rilevato un file di archivio infetto, verrà eliminato l'intero archivio, anche se sono presenti file puliti.

7.1.5.4 Esclusioni

Un'estensione è la parte del nome di un file delimitata da un punto. L'estensione definisce il tipo e il contenuto di un file. Questa sezione della configurazione dei parametri di ThreatSense consente di definire i tipi di file da escludere dal controllo.

Per impostazione predefinita, tutti i file vengono sottoposti a controllo indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dal controllo. I pulsanti + e − consentono di attivare o impedire il controllo di estensioni specifiche.

L'esclusione di file dal controllo è talvolta utile nel caso in cui il controllo di determinati tipi di file impedisca il corretto funzionamento del programma. Ad esempio, è consigliabile escludere i file *log*, *cfg* e *tmp*. Il formato corretto per inserire le estensioni dei file è il seguente:
log
cfg
tmp

7.1.5.5 Limiti

La sezione **Limiti** consente di specificare la dimensione massima degli oggetti e i livelli degli archivi nidificati sui quali eseguire il controllo:

- **Dimensioni massime:** definisce la dimensione massima degli oggetti da sottoporre a controllo. Il modulo antivirus eseguirà unicamente il controllo degli oggetti di dimensioni inferiori a quelle specificate. Si consiglia di non modificare il valore predefinito, poiché di norma non sussiste alcun motivo per farlo. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dal controllo.
- **Durata massima controllo:** definisce il valore massimo di tempo destinato al controllo di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà il controllo di un oggetto una volta raggiunto tale valore temporale, indipendentemente dal fatto che il controllo sia stato o meno completato.
- **Massimo livello di nidificazione:** specifica il livello massimo di controllo degli archivi. Si consiglia di non modificare il valore predefinito di 10; in circostanze normali, non sussiste alcun motivo per farlo. Se il controllo termina prima del tempo a causa del numero di archivi nidificati, l'archivio non verrà controllato.
- **Dimensione massima file:** questa opzione consente di specificare le dimensioni massime dei file contenuti all'interno degli archivi da sottoporre a controllo una volta estratti. Se, a causa di tale limite, il controllo termina prima del tempo, l'archivio non verrà controllato.

7.1.5.6 Altri

Attiva ottimizzazione intelligente
L'attivazione dell'Ottimizzazione intelligente consente di ottimizzare le impostazioni allo scopo di garantire il miglior livello di controllo, senza compromettere la velocità. I vari moduli di protezione eseguono il controllo in modo intelligente, utilizzando metodi differenti. L'ottimizzazione intelligente non è definita in modo rigido all'interno del prodotto. Il team di sviluppo ESET provvede costantemente all'implementazione di nuove modifiche che vengono successivamente integrate in ESET Endpoint Antivirus attraverso aggiornamenti periodici. Se l'opzione Ottimizzazione intelligente non è attivata, durante il controllo vengono applicate solo le impostazioni definite dall'utente di moduli specifici nell'architettura di ThreatSense.

Controlla flussi dati alternativi (solo per controllo su richiesta)
I flussi di dati alternativi (fork risorse/dati) utilizzati dal file system sono associazioni di file e cartelle invisibili alle tecniche di controllo standard. Numerose infiltrazioni tentano di eludere le rilevazioni presentandosi come flussi di dati alternativi.

7.1.6 Rilevamento di un'infiltrazione

Le infiltrazioni possono raggiungere il sistema da diversi punti di accesso: pagine Web, cartelle condivise, messaggi e-mail o periferiche rimovibili (USB, dischi esterni, CD, DVD e così via).

Se il computer mostra segnali di infezione da malware (ad esempio, appare più lento, si blocca spesso e così via), si consiglia di seguire le istruzioni sottostanti:

1. Fare clic su **Controllo computer**.
2. Fare clic su **Controllo intelligente** (per ulteriori informazioni, vedere la sezione Controllo intelligente 14).
3. Al termine del controllo, analizzare nel registro il numero di file sottoposti a controllo, infetti e puliti.

Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare le destinazioni nelle quali dover ricercare malware.

Per avere un'idea generale di come ESET Endpoint Antivirus gestisce le infiltrazioni, si supponga che il monitoraggio del file system in tempo reale, che utilizza il livello di pulizia predefinito, rilevi un'infiltrazione. La protezione in tempo reale tenterà di pulire o di eliminare il file. In assenza di azioni predefinite disponibili per il modulo di protezione in tempo reale, all'utente verrà chiesto di selezionare un'opzione in una finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, poiché tale opzione lascia inalterati i file infetti. Questa opzione è pensata per le situazioni in cui si è certi che il file non è pericoloso e che si tratta di un errore di rilevamento.

Pulizia ed eliminazione - Eseguire la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto un codice dannoso. In tal caso, tentare in primo luogo di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codice dannoso, verrà eliminato.

Eliminazione dei file negli archivi - In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati se anche dovessero contenere file puliti non dannosi. È consigliabile essere prudenti durante l'esecuzione di un controllo di **Massima pulizia**, poiché in questa modalità l'archivio viene eliminato anche se contiene un solo file infetto, indipendentemente dallo stato degli altri file dell'archivio.

7.2 Protezione Web e e-mail

Per accedere alla protezione Web e e-mail dal menu principale, fare clic su **Configurazione** > **Web e e-mail**. Da qui, è anche possibile accedere alle impostazioni dettagliate di ciascun modulo facendo clic su **Configurazione**.

Protezione accesso Web: monitora le comunicazioni HTTP/HTTPS tra i browser Web e i server remoti.

Protezione client di posta - garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP.

Protezione Anti-Phishing - blocca i potenziali attacchi phishing provenienti da siti Web o dai domini presenti nel database dei malware ESET.

7.2.1 Protezione accesso Web

La protezione accesso Web consiste nel controllo delle comunicazioni tra i browser Web e i server remoti per garantire la conformità alle regole HTTP (Hypertext Transfer Protocol) o HTTPS.

7.2.1.1 Porte

Nella scheda **Porte** è possibile definire i numeri delle porte utilizzate per la comunicazione HTTP. I numeri delle porte predefiniti sono 80, 8080 e 3128.

7.2.1.2 Modalità attiva

ESET Endpoint Antivirus prevede anche il sottomenu **Modalità attiva**, che definisce la modalità di controllo per i browser Web. La modalità attiva esamina i dati trasferiti dalle applicazioni che hanno accesso a Internet, indipendentemente dal fatto che siano o meno browser Web. Se questa opzione non è attivata, le comunicazioni provenienti dalle applicazioni vengono monitorate gradualmente in batch. Ciò riduce l'efficacia del processo di verifica dei dati, ma offre una maggiore compatibilità per le applicazioni elencate. Se non si verificano problemi durante l'utilizzo, è consigliabile attivare il controllo della modalità attiva selezionando la casella di controllo accanto all'applicazione desiderata.

Quando un'applicazione controllata scarica i dati, questi vengono salvati in un file temporaneo creato da ESET Endpoint Antivirus. I dati non sono disponibili per la specifica applicazione in quel momento. Una volta completato il download, i dati vengono controllati per la ricerca di codice dannoso. Se non vi sono infiltrazioni, i dati vengono inviati all'applicazione originale. Questo processo offre un controllo completo delle comunicazioni effettuate da un'applicazione controllata. Se viene attivata la modalità passiva, i dati vengono inviati in modo graduale all'applicazione originale per evitare timeout.

7.2.1.3 Elenchi URL

La sezione **Elenchi URL** consente all'utente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo. I siti Web contenuti nell'elenco di indirizzi bloccati non saranno accessibili. I siti Web contenuti nell'elenco di indirizzi esclusi sono accessibili senza dover essere controllati per la ricerca di codice dannoso.

Per accedere solo agli indirizzi URL specificati nell'elenco **URL consentiti**, selezionare **Limita indirizzi URL**.

Per attivare un elenco, selezionare **Attivato** accanto al nome. Se si desidera ricevere una notifica relativa all'inserimento di un indirizzo proveniente dall'elenco corrente, selezionare **Notificato**.

I simboli speciali *(asterisco) e ?(punto interrogativo) possono essere utilizzati durante la creazione degli elenchi di URL. L'asterisco sostituisce qualsiasi stringa di caratteri e il punto interrogativo sostituisce qualsiasi simbolo. È necessario prestare particolare attenzione quando si specificano gli indirizzi esclusi, in quanto l'elenco dovrebbe contenere esclusivamente indirizzi affidabili e sicuri. Allo stesso modo, è necessario assicurarsi che i simboli * e ? vengano utilizzati correttamente in questo elenco.

7.2.2 Protezione e-mail

La protezione e-mail garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP. Durante la verifica dei messaggi in arrivo, il programma utilizza tutti i metodi di controllo avanzato previsti nel motore di controllo ThreatSense. Ciò significa che il rilevamento di programmi dannosi avviene ancora prima del confronto con il database delle firme antivirali. Il controllo delle comunicazioni mediante i protocolli POP3 e IMAP è indipendente dal client di posta utilizzato.

Motore ThreatSense - la configurazione avanzata dello scanner antivirus consente di configurare le destinazioni di controllo, i metodi di rilevamento e così via. Fare clic su **Configurazione** per visualizzare la finestra della configurazione dettagliata dello scanner.

Dopo che un'e-mail è stata controllata, è possibile aggiungere al messaggio una notifica contenente i risultati del controllo. È possibile selezionare **Aggiungi notifiche all'oggetto di un'e-mail**. Poiché potrebbero essere omesse in messaggi HTML problematici oppure create da alcuni virus, non è possibile creare notifiche che non contengono una domanda. Sono disponibili le seguenti opzioni:

Mai - non verrà aggiunta alcuna notifica,
Solo per l'e-mail infetta - verranno contrassegnati come controllati solo i messaggi contenenti un software dannoso,
Per tutte le e-mail controllate - il programma aggiungerà messaggi a tutte le e-mail controllate.

Modello aggiunto all'oggetto di un'e-mail infetta - modificare questo modello per cambiare il formato del prefisso dell'oggetto di un'e-mail infetta.

Aggiungi notifica alla nota a piè di pagina di un'e-mail - attivare questa casella di controllo se si desidera che la protezione e-mail aggiunga un allarme virus all'e-mail infetta. Questa funzione consente di eseguire un semplice filtraggio delle e-mail infette e. di aumentare il livello di credibilità del destinatario. Inoltre, in caso di rilevamento di un'infiltrazione, fornisce informazioni preziose relative al livello di minaccia di e-mail o mittenti specifici.

7.2.2.1 Verifica del protocollo POP3

Il protocollo POP3 è il protocollo più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client di posta. ESET Endpoint Antivirus offre protezione per questo protocollo, indipendentemente dal client di posta utilizzato.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Assicurarsi che il modulo sia attivato per garantire un corretto funzionamento del filtraggio protocolli. Il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono controllate tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

Selezionando **Attiva verifica protocollo POP3**, tutto il traffico POP3 viene monitorato per rilevare il software dannoso.

7.2.2.2 Verifica del protocollo IMAP

Il protocollo di accesso ai messaggi Internet (IMAP) è un altro protocollo Internet per il recupero delle e-mail. Il protocollo IMAP offre alcuni vantaggi rispetto al protocollo POP3, tra cui, ad esempio, la possibilità di connettere simultaneamente più di un client alla stessa casella di posta e conservare informazioni sullo stato dei messaggi (lettura, invio di risposta o eliminazione). ESET Endpoint Antivirus offre protezione per questo protocollo, indipendentemente dal client di posta utilizzato.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Assicurarsi che il controllo del protocollo IMAP sia attivato per garantire un corretto funzionamento del modulo. Il controllo del protocollo IMAP viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono controllate tutte le comunicazioni della porta 143, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

Selezionando **Attiva verifica protocollo IMAP**, tutto il traffico IMAP viene monitorato per rilevare il software dannoso.

7.3 Anti-Phishing

Il termine *phishing* definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti allo scopo di ottenere informazioni riservate). Il phishing viene spesso utilizzato per ottenere l'accesso a dati sensibili, quali numeri di conti bancari, numeri di carte di credito, codici PIN oppure nomi utente e password.

Si consiglia di mantenere attivata la funzione Anti-Phishing (**Configurazione** > **Inserisci preferenze applicazione...** > **Protezione Anti-Phishing**). I potenziali attacchi di phishing provenienti dai siti Web o dai domini presenti nel database dei malware ESET, per i quali l'utente riceverà una notifica, verranno bloccati.

8. Controllo dispositivi

ESET Endpoint Antivirus consente di controllare, bloccare o regolare le estensioni dei filtri e/o delle autorizzazioni e di definire la capacità di un utente di accedere e di utilizzare un determinato dispositivo. Questa funzionalità è utile nel caso in cui l'amministratore di un computer desideri impedire l'utilizzo di dispositivi con contenuti non desiderati.

Dispositivi esterni supportati:
- Archiviazione su disco (HDD, memoria USB)
- CD/DVD
- Stampante USB
- Dispositivo di acquisizione immagini
- Porta seriale
- Rete
- Dispositivo portatile

In caso di inserimento di un dispositivo bloccato mediante una regola esistente, verrà visualizzata una finestra di notifica e l'accesso al dispositivo non verrà concesso.

Il rapporto Controllo dispositivi registra tutte le occorrenze di attivazione del controllo dispositivi. Le voci del rapporto possono essere visualizzate nella finestra principale del programma di ESET Endpoint Antivirus in **Strumenti** > **File di rapporto** 22.

8.1 Editor regole

Le opzioni di configurazione del controllo dispositivi possono essere modificate in **Configurazione** > **Inserisci preferenze applicazione...** > **Controllo dispositivi**.

Fare clic su **Attiva controllo dispositivi** per attivare la funzione Controllo dispositivi in ESET Endpoint Antivirus. Dopo aver attivato il Controllo dispositivi, è possibile gestire e modificare i ruoli del Controllo dispositivi. Selezionare la casella di controllo accanto al nome di una regola per attivarla e disattivarla.

Utilizzare i pulsanti + o − per aggiungere o rimuovere le regole. Le regole sono disposte in ordine di priorità, partendo da quelle con priorità più elevata. Per modificare l'ordine, selezionare una regola e trascinarla nella nuova posizione oppure fare clic su e scegliere una delle opzioni.

ESET Endpoint Antivirus rileva automaticamente tutti i dispositivi attualmente inseriti e i relativi parametri (tipo di dispositivo, fornitore, modello, numero di serie). Anziché creare le regole manualmente, fare clic sull'opzione **Popola**, selezionare il dispositivo e fare clic su **Continua** per creare la regola.

È possibile consentire o bloccare specifici dispositivi in base all'utente, al gruppo di utenti o a uno qualsiasi dei vari parametri aggiuntivi che è possibile specificare nella configurazione delle regole. L'elenco delle regole contiene varie descrizioni tra cui nome, tipo di dispositivo, gravità di registrazione e azione da eseguire dopo aver collegato un dispositivo al computer.

Nome
Inserire una descrizione della regola nel campo **Nome** per consentire una migliore identificazione. La casella di controllo **Regola attivata** consente di disattivare o attivare questa regola. Questa opzione può essere utile se non si desidera eliminare definitivamente la regola.

Tipo di dispositivo
Selezionare il tipo di dispositivo esterno desiderato nel menu a discesa. Le informazioni sul tipo di dispositivo sono raccolte dal sistema operativo. I supporti di archiviazione includono dischi esterni o lettori tradizionali di schede di memoria collegati tramite USB o FireWire. Per lettori di smart card si intendono dispositivi in grado di leggere qualsiasi supporto con un circuito integrato incorporato, come ad esempio schede SIM o schede di autenticazione. Esempi di dispositivi di acquisizione immagini sono gli scanner o le fotocamere. Poiché tali dispositivi non forniscono informazioni sugli utenti, ma solo sulle azioni, possono essere bloccati solo a livello globale.

Azione
È possibile consentire o bloccare l'accesso ai dispositivi non adatti all'archiviazione. Le regole dei dispositivi di archiviazione consentono invece all'utente di scegliere uno dei seguenti diritti:
Lettura/Scrittura: sarà consentito l'accesso completo al dispositivo
Solo lettura: sul dispositivo sarà consentito l'accesso di sola lettura
Blocca: l'accesso al supporto verrà bloccato

Tipo di criterio
Selezionare **Gruppo dispositivi** o **Dispositivo**. I parametri aggiuntivi visualizzati di seguito possono essere utilizzati per ottimizzare le regole e personalizzarle in base ai dispositivi in uso.
Fornitore: filtraggio in base al nome o all'identificativo del fornitore
Modello: nome specifico del dispositivo
Numero di serie: generalmente, a ogni dispositivo esterno è associato un numero di serie. Nel caso di CD/DVD, il numero di serie è associato al supporto specifico e non all'unità CD/DVD

NOTA: se i parametri non sono definiti, la regola ignorerà questi campi durante la ricerca delle corrispondenze. I parametri di filtraggio in tutti i campi testuali non fanno distinzione tra maiuscole e minuscole e i caratteri jolly (*, ?) non sono supportati.

SUGGERIMENTO: per visualizzare le informazioni relative a un dispositivo, creare una regola per quello specifico dispositivo e collegare il dispositivo al computer in uso. Dopo aver collegato il dispositivo, i relativi dettagli saranno visualizzati nel Rapporto controllo dispositivi 22.

Gravità registrazione
Sempre: registra tutti gli eventi

Diagnostica: registra le informazioni necessarie ai fini dell'ottimizzazione del programma
Informazioni: registra i messaggi informativi, compresi tutti i record indicati in precedenza
Avvisi: consente di registrare errori critici e messaggi di allarme
Nessuno: non verrà registrato alcun rapporto

Elenco utente

Le regole possono essere limitate a determinati utenti o gruppi di utenti aggiunti all'Elenco utenti:
Modifica...: consente di aprire l'**Editor identità** dove è possibile selezionare utenti o gruppi. Per definire un elenco di utenti, selezionarli nell'elenco **Utenti** sul lato sinistro e fare clic su **Aggiungi**. Per rimuovere un utente, selezionarne il nome nell'elenco **Utenti selezionati** e fare clic su **Rimuovi**. Per visualizzare tutti gli utenti del sistema, selezionare **Mostra tutti gli utenti**. Se l'elenco è vuoto, tutti gli utenti saranno consentiti

NOTA: non tutti i dispositivi possono essere filtrati dalle regole dell'utente (ad esempio, i dispositivi di acquisizione di immagini non forniscono informazioni sugli utenti, ma solo sulle azioni).

9. Strumenti

Il menu **Strumenti** contiene moduli che semplificano l'amministrazione del programma e offrono opzioni aggiuntive agli utenti avanzati.

9.1 File di rapporto

I file di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta uno strumento essenziale per l'analisi del sistema, il rilevamento delle minacce e la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET Endpoint Antivirus, nonché dall'archivio dei rapporti.

È possibile accedere ai file di rapporto dal menu principale di ESET Endpoint Antivirus facendo clic su **Strumenti** > **File di rapporto**. Selezionare il tipo di rapporto desiderato utilizzando il menu a discesa **Rapporto** nella parte superiore della finestra. Sono disponibili i seguenti rapporti:

1. **Minacce rilevate**: informazioni sugli eventi relativi al rilevamento delle infiltrazioni.
2. **Eventi**: tutte le azioni importanti eseguite da ESET Endpoint Antivirus vengono registrate nei rapporti degli eventi.
3. **Controllo computer** - In questa finestra vengono visualizzati i risultati di tutti i controlli completati. Fare doppio clic su una voce qualsiasi per visualizzare i dettagli di un controllo del computer specifico.
4. **Controllo dispositivi**: contiene record relativi ai supporti rimovibili o ai dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con una regola di controllo dispositivi. Se la regola non corrisponde a un dispositivo collegato, non verrà creata alcuna voce di rapporto relativa a tale evento. Qui è possibile visualizzare anche dettagli relativi al tipo di dispositivo, numero di serie, nome del fornitore e dimensioni del supporto (se disponibili).
5. **Siti Web filtrati**: questo elenco è utile se si desidera visualizzare un elenco di siti Web che sono stati bloccati dalla Protezione accesso Web 18. In questi rapporti è possibile visualizzare l'ora, l'indirizzo URL, lo stato, l'indirizzo IP, l'utente e l'applicazione che hanno aperto una connessione a un sito Web specifico.

Fare clic con il pulsante destro del mouse su un file di rapporto qualsiasi e fare clic su **Copia** per copiare i contenuti di quel file di rapporto negli Appunti.

9.1.1 Manutenzione rapporto

La configurazione della registrazione di ESET Endpoint Antivirus è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Inserisci preferenze applicazione...** > **Strumenti** > **File di rapporto**. È possibile specificare le opzioni seguenti per i file di rapporto:

- **Elimina automaticamente i file di rapporto** - le voci del rapporto con data precedente al numero di giorni specificato vengono automaticamente eliminate.
- **Ottimizza automaticamente i file di rapporto** - i file di rapporto vengono automaticamente deframmentati se viene superata la percentuale specificata di record inutilizzati.

È possibile salvare tutte le informazioni rilevanti visualizzate nell'interfaccia utente grafica, nonché i messaggi relativi alle minacce e agli eventi, in formati di testo leggibili, come testo normale o CSV (valori separati da virgola). Se si desidera elaborare questi file mediante strumenti di terze parti, selezionare la casella di controllo accanto a **Attiva registrazione a file di testo**.

Per definire la cartella di destinazione in cui verranno salvati i file di rapporto, fare clic su **Configurazione** accanto a **Configurazione avanzata**.

Le opzioni presenti nella sezione **File di testo dei rapporti:** sono: **Modifica**, che consente di salvare i rapporti inserendo le seguenti informazioni:

- Alcuni eventi tra cui *Nome utente e password non validi*, *Non è possibile aggiornare il database delle firme antivirali*, ecc. sono indicati nel file *eventslog.txt*.
- Le minacce rilevate dal Controllo all'avvio, dalla Protezione in tempo reale o dal Controllo computer sono salvate nel file chiamato *threatslog.txt*.
- I risultati di tutti i controlli completati vengono salvati nel formato *scanlog.NUMERO.txt*.
- I dispositivi bloccati dal Controllo dispositivi vengono menzionate in devctllog.txt

Per configurare i filtri per i **Record predefiniti rapporti controllo computer**, fare clic su **Modifica** e selezionare/deselezionare i tipi di rapporto in base alle specifiche esigenze. Per ulteriori informazioni su questi tipi di rapporto, consultare Filtraggio rapporti 23.

9.1.2 Filtraggio rapporti

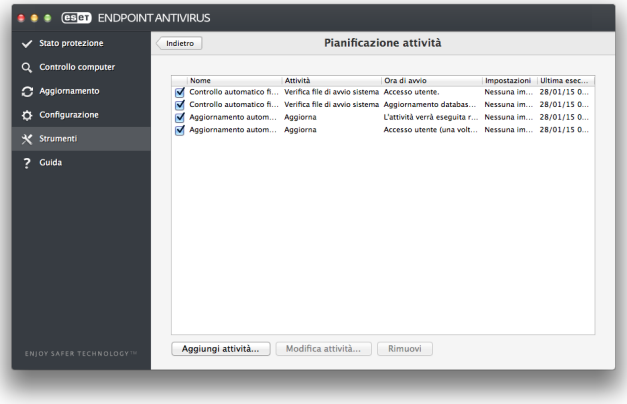
I rapporti memorizzano le informazioni relative a eventi importanti di sistema. La funzione di filtraggio del rapporto consente di visualizzare i record di eventi specifici.

I tipi di rapporto utilizzati più spesso sono elencati di seguito:

- **Allarmi critici** - errori critici di sistema (ad esempio, Impossibile avviare la protezione antivirus)
- **Errori** - messaggi di errore come " *Errore durante il download del file*" ed errori critici
- **Allarmi** - messaggi di allarme
- **Record informativi** - messaggi informativi che includono gli aggiornamenti riusciti, gli avvisi e così via.
- **Record diagnostici** - informazioni necessarie per la sincronizzazione del programma, nonché di tutti i record riportati sopra.

9.2 Pianificazione attività

È possibile trovare la **Pianificazione attività** nel menu principale di ESET Endpoint Antivirus sotto a **Strumenti**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, come data, ora e profilo di controllo predefiniti utilizzati.



La Pianificazione attività consente di gestire e avviare attività pianificate con le configurazioni e le proprietà predefinite. La configurazione e le proprietà contengono informazioni quali la data e l'ora, oltre ai profili specificati da utilizzare durante l'esecuzione dell'attività.

Per impostazione predefinita, in Pianificazione attività vengono visualizzate le seguenti attività pianificate:

- Manutenzione rapporto (dopo aver attivato **Mostra attività di sistema** nella configurazione della pianificazione attività)
- Controllo file di avvio dopo l'accesso dell'utente
- Controllo file di avvio dopo il completamento dell'aggiornamento del database delle firme antivirali
- Aggiornamento automatico periodico
- Aggiornamento automatico dopo l'accesso dell'utente

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), premere il pulsante CTRL, fare clic sull'attività che si desidera modificare e selezionare **Modifica** oppure l'attività e fare clic su **Modifica attività**.

9.2.1 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic su **Aggiungi attività** oppure su CTRL e su un campo vuoto e selezionare **Aggiungi** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione**
- **Aggiorna**
- **Manutenzione rapporto**
- **Controllo del computer su richiesta**
- **Controllo del file di avvio del sistema**

NOTA: scegliendo **Esegui applicazione**, è possibile eseguire i programmi come utente del sistema "nessuno". Le autorizzazioni per l'esecuzione delle applicazioni mediante la Pianificazione attività sono definite dal sistema operativo Mac OS X.

Nell'esempio sottostante, verrà utilizzata la Pianificazione attività per aggiungere una nuova attività di aggiornamento, che rappresenta una delle attività pianificate usate con maggiore frequenza:

1. Selezionare **Aggiorna** dal menu a discesa **Attività pianificata**.
2. Digitare un nome per l'attività nel campo **Nome attività**.
3. Selezionare la frequenza dell'attività dal menu a discesa **Esegui attività**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento. Se si seleziona **Definito dall'utente**, verrà richiesto di specificare la data/l'ora in formato *cron* (per ulteriori informazioni, consultare la sezione Creazione di un'attività definita dall'utente 24).
4. Nella fase successiva, è possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati.
5. Fare clic su **Fine**. La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

Per impostazione predefinita, ESET Endpoint Antivirus contiene attività pianificate predefinite per garantire il corretto funzionamento del sistema. Poiché tali attività non devono essere modificate, sono nascoste per impostazione predefinita. Per rendere visibili queste attività, dal menu principale fare clic su **Configurazione** > **Inserisci preferenze applicazione** > **Pianificazione attività** e selezionare **Mostra attività di sistema**.

9.2.2 Creazione di un'attività definita dall'utente

Quando si seleziona il tipo di attività Definita dall'utente dal menu a discesa Esegui attività, è necessario definire alcuni parametri speciali.

È necessario inserire la data e l'ora di un'attività **Definita dall'utente** in formato cronologico con l'anno esteso (stringa che comprende 6 campi separati da uno spazio bianco):

```
minuto (0-59) ora (0-23) giorno del mese (1-31)
mese (1-12) anno (1970-2099) giorno della
settimana (0-7) (domenica = 0 o 7)
```

Ad esempio:

```
30 6 22 3 2012 4
```

I seguenti caratteri speciali sono supportati nelle espressioni cronologiche:

- asterisco (`*`) - l'espressione corrisponderà a tutti i valori del campo, ad es. l'asterisco nel 3° campo (giorno del mese) indica ogni giorno
- trattino (-) - definisce gli intervalli, ad es. `3-9`
- virgola (,) - separa gli elementi di un elenco, ad es. `1,3,7,8`
- barra (`/`) - definisce gli incrementi degli intervalli, ad es. `3-28/5` nel 3° campo (giorno del mese) indica il 3° giorno del mese e successivamente ogni 5 giorni.

I nomi dei giorni (Monday-Sunday) e dei mesi (January-December) non sono supportati.

NOTA: se si definiscono sia il giorno del mese sia il giorno della settimana, il comando verrà eseguito sono in caso di corrispondenza di entrambi i campi.

9.3 Live Grid

Il Sistema di allarme immediato Live Grid è uno strumento in grado di informare ESET in modo immediato e costante sulle nuove infiltrazioni. Il sistema di allarme immediato bidirezionale Live Grid è stato concepito con un unico scopo: migliorare la sicurezza degli utenti. Il sistema migliore per garantire il rilevamento di nuove minacce subito dopo la loro comparsa consiste nell'effettuare il "collegamento" al maggior numero di clienti possibile e nell'utilizzo delle informazioni raccolte per garantire un aggiornamento costante dei dati relativi alle firme antivirali. Selezionare una delle opzioni per Live Grid:

1. Si può scegliere di non attivare il sistema di allarme immediato Live Grid. Non verrà persa alcuna funzionalità del software, ma, in alcuni casi, ESET Endpoint Antivirus potrebbe rispondere più rapidamente alle nuove minacce rispetto all'aggiornamento del database delle firme antivirali.
2. È possibile configurare il sistema di allarme immediato Live Grid per inviare informazioni anonime relative alle nuove minacce e alle posizioni del nuovo codice di minaccia. Queste informazioni possono essere inviate a ESET per un'analisi dettagliata. L'analisi di tali minacce consentirà a ESET di aggiornare il database di minacce e di potenziare le capacità di rilevamento delle minacce.

Il sistema di allarme immediato Live Grid raccoglierà informazioni sul computer correlate alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso al file, il nome del file, informazioni su data e ora, il processo in base al quale la minaccia è apparsa sul computer e le informazioni sul sistema operativo del computer.

Sebbene sia possibile che tale sistema riveli occasionalmente alcune informazioni relative all'utente o al computer in uso (nomi utente in un percorso di directory e così via) al laboratorio delle minacce ESET, tali dati verranno utilizzati ESCLUSIVAMENTE per consentire al sistema di rispondere immediatamente alle nuove minacce.

Per accedere alla configurazione di Live Grid dal menu principale, fare clic su **Configurazione** > **Inserisci preferenze applicazione** > **Live Grid**. Selezionare **Attiva il sistema di reputazione ESET Live Grid (scelta consigliata)** per attivare Live Grid, quindi fare clic su **Configurazione** accanto a **Opzioni avanzate**.

9.3.1 File sospetti

Per impostazione predefinita, ESET Endpoint Antivirus viene configurato per l'invio di file sospetti al laboratorio delle minacce ESET per l'analisi dettagliata. Se non si desidera inviare questi file automaticamente, deselezionare **Invio di file sospetti** (**Configurazione** > **Inserisci preferenze applicazione** > **Live Grid** > **Configura**).

Se si rileva un file sospetto, è possibile inviarlo al laboratorio delle minacce ESET per l'analisi. Per eseguire questa operazione, fare clic su **Strumenti** > **Invia file per analisi** dalla finestra principale del programma. Se viene individuata un'applicazione dannosa, la sua firma verrà aggiunta al successivo aggiornamento delle firme antivirali.

Invio di informazioni statistiche anonime - Il Sistema di allarme immediato ESET Live Grid raccoglie informazioni in forma anonima sul computer correlate alle minacce rilevate di recente. Queste informazioni comprendono il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione del prodotto di protezione ESET, la versione del sistema operativo in uso e le impostazioni di ubicazione. In genere, le statistiche vengono inviate ai server ESET una o due volte al giorno.

Di seguito è riportato un esempio di pacchetto di statistiche inviato:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

Filtro di esclusione - Questa opzione consente di escludere dall'invio determinati tipi di file. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo. I tipi di file più comuni sono esclusi per impostazione predefinita (.doc, .rtf e così via). È possibile aggiungere qualunque tipologia di file alla lista degli elementi esclusi.

Indirizzo e-mail del contatto (facoltativo) - L'indirizzo e-mail dell'utente sarà utilizzato qualora sia necessario ottenere ulteriori informazioni ai fini dell'analisi. È importante notare che l'utente non riceverà una risposta da ESET, a meno che non siano richieste ulteriori informazioni.

9.4 Quarantena

Lo scopo principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o se vengono erroneamente rilevati come minacce da ESET Endpoint Antivirus.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati al laboratorio delle minacce ESET per l'analisi.

I file salvati nella cartella di quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo della quarantena (ad esempio, aggiunto dall'utente) e il numero di minacce rilevate. La cartella quarantena (*/Library/Application Support/Eset/esets/cache/quarantine*) rimane nel sistema anche dopo aver disinstallato ESET Endpoint Antivirus. I file in quarantena sono archiviati in un formato sicuro crittografato e possono essere ripristinati dopo l'installazione di ESET Endpoint Antivirus.

9.4.1 Mettere file in quarantena

ESET Endpoint Antivirus mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto a deselezionare questa opzione nella finestra di avviso). Dalla finestra Quarantena, è possibile fare clic su Quarantena per aggiungere manualmente un file qualsiasi alla quarantena. È inoltre possibile fare clic e premere contemporaneamente il pulsante Ctrl su un file in qualsiasi momento e selezionare Servizi > ESET Endpoint Antivirus - Aggiungere i file alla quarantena dal menu contestuale per inviarli alla quarantena.

9.4.2 Ripristino di un file in quarantena

I file messi in quarantena possono anche essere ricollocati nella loro posizione originale. Per far ciò, selezionare un file messo in quarantena e fare clic su **Ripristina**. Il ripristino è anche disponibile dal menu contestuale, premendo CTRL, selezionando un dato file nella finestra Quarantena e facendo clic su **Ripristina**. È possibile utilizzare **Ripristina in** per collocare un file in una posizione diversa da quella dalla quale è stato messo in quarantena.

9.4.3 Invio di un file dalla quarantena

Se è stato messo in quarantena un file sospetto che non è stato rilevato dal programma o se un file è stato valutato erroneamente come infetto (ad esempio, da un'analisi euristica del codice) e quindi messo in quarantena, inviare il file al laboratorio delle minacce ESET. Per inviare un file dalla quarantena, premere CTRL, fare clic sul file e selezionare **Invia per analisi** dal menu contestuale.

9.5 Privilegi

Le impostazioni di ESET Endpoint Antivirus rivestono un ruolo fondamentale dal punto di vista dei criteri di sicurezza di un'azienda. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Di conseguenza, è possibile scegliere quali utenti potranno modificare la configurazione del programma.

È possibile configurare gli utenti con privilegi sotto a **Configurazione** > **Inserisci preferenze applicazione** > **Utente** > **Privilegi**.

Per garantire la massima protezione del sistema, è necessario configurare correttamente il programma. Qualsiasi modifica non autorizzata può provocare la perdita di dati importanti. Per definire un elenco di utenti con privilegi, selezionarli dalla lista **Utenti** sul lato sinistro e fare clic su **Aggiungi**. Per rimuovere un utente, selezionarne il nome nell'elenco **Utenti con privilegi** sul lato destro e fare clic su **Rimuovi**. Per visualizzare tutti gli utenti del sistema, selezionare **Mostra tutti gli utenti**.

NOTA: se l'elenco di utenti con privilegi è vuoto, tutti gli utenti del sistema saranno autorizzati a modificare le impostazioni del programma.

9.6 Modalità presentazione

La **Modalità presentazione** è una funzionalità pensata per gli utenti che richiedono un utilizzo ininterrotto del software, non vogliono essere disturbati dalle finestre popup e desiderano ridurre al minimo l'utilizzo della CPU. La modalità presentazione può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività antivirus. Se attivata, tutte le finestre popup verranno disattivate e le attività pianificate non verranno eseguite. La protezione del sistema è ancora in esecuzione in background, ma non richiede l'interazione dell'utente.

Per attivare manualmente la modalità presentazione, fare clic su **Configurazione** > **Inserisci preferenze applicazione...** > **Modalità presentazione** > **Attiva modalità presentazione**.

Selezionare la casella di controllo accanto a **Attiva automaticamente modalità Presentazione in modalità a schermo intero** per attivare automaticamente la modalità presentazione nel momento in cui le applicazioni sono in modalità a schermo intero. In caso di attivazione di questa funzione, la modalità presentazione si attiverà all'avvio di un'applicazione in modalità a schermo intero e si interromperà automaticamente all'uscita dall'applicazione. Questa funzionalità si rivela particolarmente utile per l'avvio di una presentazione.

È inoltre possibile selezionare **Disattiva automaticamente modalità Presentazione dopo** per definire l'intervallo di tempo espresso in minuti dopo il quale la modalità presentazione verrà automaticamente disattivata.

L'attivazione della modalità presentazione rappresenta un potenziale rischio per la protezione. Per tale motivo, l'icona relativa allo stato di protezione di ESET Endpoint Antivirus diventa di colore arancione e viene visualizzato un avviso.

9.7 Processi in esecuzione

L'elenco di **Processi in esecuzione** contiene i processi in esecuzione sul computer in uso. ESET Endpoint Antivirus fornisce informazioni dettagliate sui processi in esecuzione allo scopo di garantire la protezione degli utenti mediante l'utilizzo della tecnologia ESET Live Grid.

- **Processo** - nome del processo attualmente in esecuzione sul computer in uso. È inoltre possibile utilizzare il Monitoraggio attività (disponibile in */ Applications/Utilities*) per visualizzare tutti i processi in esecuzione sul computer dell'utente.
- **Livello di rischio** - nella maggior parte dei casi, ESET Endpoint Antivirus e la tecnologia ESET Live Grid assegnano livelli di rischio agli oggetti (file, processi e così via) utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto analizzandone il potenziale relativo all'attività dannosa. Agli oggetti viene assegnato un livello di rischio sulla base di queste regole euristiche. Le applicazioni note contrassegnate di verde sono definitivamente pulite (inserite nella whitelist) e saranno escluse dal controllo. Tale operazione migliora la velocità sia dei controlli su richiesta sia dei controlli in tempo reale. Se un'applicazione è contrassegnata come sconosciuta (in giallo), non si tratta necessariamente di software dannoso. In genere, si tratta semplicemente di un'applicazione più recente. In caso di dubbi relativi a un file, è possibile inviarlo al laboratorio delle minacce ESET per l'analisi. Se il file si rivela essere un'applicazione dannosa, la sua firma verrà aggiunta in un aggiornamento successivo.
- **Numero di utenti** - numero di utenti che utilizzano una data applicazione. Queste informazioni vengono raccolte mediante la tecnologia ESET Live Grid.
- **Orario del rilevamento** - periodo di tempo dal rilevamento dell'applicazione da parte della tecnologia ESET Live Grid.
- **ID bundle applicazione** - nome del fornitore o del processo di applicazione.

Facendo clic su un dato processo, appariranno le seguenti informazioni nella parte inferiore della finestra:

- **File** - posizione di un'applicazione nel computer in uso
- **Dimensioni file** - dimensione fisica del file sul disco
- **Descrizione file** - caratteristiche del file basate sulla descrizione del sistema operativo
- **ID bundle applicazione** - nome del fornitore o del processo di applicazione

- **Versione file** - informazioni provenienti dal pubblicatore dell'applicazione
- **Nome prodotto** - nome dell'applicazione e/o ragione sociale

10. Interfaccia utente

Le opzioni di configurazione dell'interfaccia utente consentono all'utente di modificare l'ambiente di lavoro per adattarlo alle sue specifiche esigenze. È possibile accedere a tali opzioni dal menu principale facendo clic su **Configurazione** > **Inserisci preferenze applicazione** > **Interfaccia**.

- Per visualizzare la schermata iniziale di ESET Endpoint Antivirus all'avvio del sistema, selezionare **Mostra schermata iniziale all'avvio**.
- **Presenta applicazione in dock** consente all'utente di visualizzare l'icona ⓔ di ESET Endpoint Antivirus nel dock del sistema operativo Mac e di passare da ESET Endpoint Antivirus ad altre applicazioni in esecuzione e viceversa premendo *cmd-tab*. Le modifiche avranno effetto al riavvio di ESET Endpoint Antivirus (attivato generalmente dal riavvio del computer).
- **Utilizza menu standard** consente di utilizzare alcuni tasti di scelta rapida (vedere Tasti di scelta rapida 10) e di visualizzare voci del menu standard (Interfaccia utente, Configurazione e Strumenti) sulla barra dei menu del sistema operativo MAC (nella parte superiore della schermata).
- Attivare **Mostra descrizioni comandi** per visualizzare le descrizioni dei comandi quando si posiziona il cursore su alcune opzioni in ESET Endpoint Antivirus.
- **Mostra file nascosti** consente all'utente di visualizzare e selezionare i file nascosti nella configurazione **Destinazioni di controllo** per un **Controllo computer**.

10.1 Avvisi e notifiche

La sezione **Avvisi e notifiche** consente di configurare la gestione degli avvisi delle minacce e delle notifiche di sistema da parte di ESET Endpoint Antivirus.

La disattivazione di **Visualizza avvisi** disattiverà tutte le finestre di avviso ed è pertanto raccomandata solo per situazioni specifiche. Nella maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).

La selezione di **Visualizza notifiche sul desktop** consentirà di visualizzare sul desktop le finestre di avviso che non richiedono l'interazione da parte dell'utente (per impostazione predefinita, l'angolo in alto a destra dello schermo). È possibile definire il periodo durante il quale verrà visualizzata una notifica modificando il valore **Chiudi automaticamente notifiche dopo** X **secondi**.

10.1.1 Configurazione avanzata avvisi e notifiche

ESET Endpoint Antivirus consente di visualizzare le finestre di dialogo degli avvisi che informano l'utente in merito a nuove versioni del programma, agli aggiornamenti del sistema operativo, alla disattivazione di alcuni componenti del programma, all'eliminazione dei rapporti e così via. È possibile rimuovere ciascuna notifica individualmente selezionando **Non mostrare nuovamente questa finestra di dialogo**.

Elenco di finestre di dialogo (**Configurazione** > **Inserisci preferenze applicazione...** > **Avvisi e notifiche** > **Configurazione**) consente di visualizzare l'elenco di tutte le finestre di dialogo attivate da ESET Endpoint Antivirus. Per attivare o eliminare ciascuna notifica, selezionare la casella di controllo sulla sinistra di **Nome finestra dialogo**. È possibile inoltre definire le **Condizioni di visualizzazione** in base alle quali verranno visualizzate le notifiche relative a nuove versioni del programma e agli aggiornamenti del sistema operativo.

10.2 Menu contestuale

Per rendere le funzioni di ESET Endpoint Antivirus disponibili dal menu contestuale, fare clic su **Configurazione** > **Inserisci preferenze applicazione** > **Menu contestuale** e selezionare la casella di controllo accanto a **Integra nel menu contestuale**. Le modifiche saranno effettive dopo l'uscita dell'utente o al riavvio del computer. Le opzioni del menu contestuale saranno disponibili sul desktop e nella finestra del **Finder**, facendo clic su CTRL e su un file o cartella qualsiasi.

11. Aggiorna

Per garantire il massimo livello di protezione, è necessario aggiornare periodicamente ESET Endpoint Antivirus. Il modulo di aggiornamento garantisce l'aggiornamento costante del programma grazie alla possibilità di scaricare il database delle firme antivirali più recente.

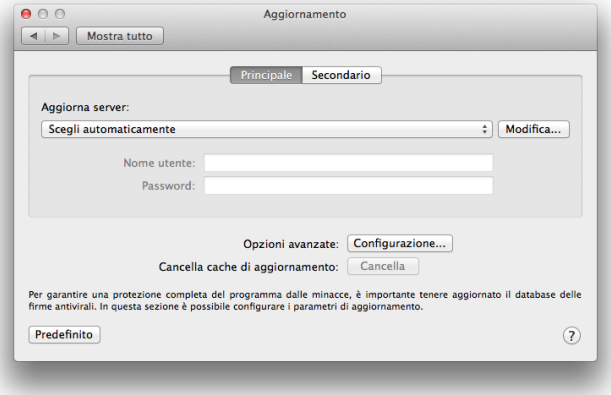
Fare clic su **Aggiorna** dal menu principale per visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente, e valutare l'eventuale necessità di eseguire un aggiornamento. Per avviare il processo di aggiornamento manualmente, fare clic su **Aggiorna database delle firme antivirali**.

In circostanze normali, ovvero in caso di download corretto degli aggiornamenti, verrà visualizzato il messaggio *Non sono necessari aggiornamenti - il database delle firme antivirali installato è aggiornato* nella finestra Aggiornamento in presenza del più recente database delle firme antivirali. Se non è possibile aggiornare il database delle firme antivirali, si raccomanda di verificare le impostazioni di aggiornamento 29: la causa più frequente di questo errore è l'immissione errata di dati sulla licenza 9 o la configurazione errata delle impostazioni di connessione 31.

La finestra **Aggiornamento** contiene anche informazioni relative alla versione del database delle firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito Web ESET in cui vengono visualizzate tutte le firme antivirali aggiunte in un dato aggiornamento.

11.1 Configurazione dell'aggiornamento

La sezione Configurazione dell'aggiornamento consente di specificare informazioni sull'origine dell'aggiornamento, come i server di aggiornamento e i dati per l'autenticazione di tali server. Per impostazione predefinita, il menu a discesa **Server di aggiornamento** è impostato su **Scegli automaticamente** per garantire che i file di aggiornamento verranno scaricati automaticamente dal server ESET con meno traffico di rete.



L'elenco dei server di aggiornamento disponibili è accessibile tramite il menu a discesa **Server di aggiornamento**. Per aggiungere un nuovo server di aggiornamento, fare clic su **Modifica**, inserire l'indirizzo del nuovo server nel campo di inserimento **Server di aggiornamento** e fare clic su **Aggiungi**.

ESET Endpoint Antivirus consente di impostare un server di aggiornamento alternativo o di failover. Il server **primario** potrebbe corrispondere al server mirror e il **Server** secondario al server di aggiornamento ESET standard. Il server secondario deve essere diverso da quello primario, altrimenti non sarà utilizzato. Se non si specificano il server di aggiornamento secondario, il nome utente e la password, l'aggiornamento di failover non funzionerà. È inoltre possibile selezionare Scegli automaticamente su e inserire il nome utente e la password nei campi appropriati per consentire a ESET Endpoint Antivirus di selezionare automaticamente il server di aggiornamento migliore da utilizzare.

In caso di problemi durante il download degli aggiornamenti del database delle firme antivirali, fare clic su Cancella **cache aggiornamento** per eliminare i file di aggiornamento temporanei.

11.1.1 Configurazione avanzata

Per disattivare le notifiche visualizzate al termine di un aggiornamento eseguito correttamente, selezionare **Non visualizzare notifiche relative agli aggiornamenti avvenuti con successo**.

Attivare gli aggiornamenti pre-rilascio per scaricare moduli di sviluppo in fase di verifica finale. Gli aggiornamenti pre-rilascio contengono spesso correzioni ai problemi del prodotto. Gli aggiornamenti ritardati consentono di scaricare gli aggiornamenti alcune ore dopo che vengono rilasciati, per assicurare che i client non ricevano aggiornamenti fino a quando viene confermato che sono privi di qualsiasi problema.

ESET Endpoint Antivirus registra gli snapshot del database delle firme antivirali e dei moduli del programma da utilizzare con la funzione **Rollback aggiornamento**. Lasciare **Crea snapshot dei file di aggiornamento** attivato per consentire a ESET Endpoint Antivirus di registrare automaticamente questi snapshot. Se si sospetta che un nuovo aggiornamento del database delle firme antivirali e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati in caso di rimando indefinito da parte dell'utente. Per ripristinare lo stato precedente di un aggiornamento, utilizzare il menu a discesa Imposta periodo di sospensione su per specificare il periodo di tempo per il quale si desidera sospendere gli aggiornamenti. Selezionando Fino alla revoca, gli aggiornamenti normali non riprenderanno finché non verranno ripristinati manualmente. Prestare la massima attenzione quando si seleziona questa impostazione.

Imposta automaticamente l'età massima del database: consente di impostare il tempo massimo (in giorni) dopo il quale il database delle firme antivirali verrà segnalato come obsoleto. Il valore predefinito è 7 giorni.

11.2 Come creare attività di aggiornamento

Fare clic su Aggiornamento > **Aggiorna database delle firme antivirali** per attivare manualmente un aggiornamento del database delle firme antivirali.

Gli aggiornamenti possono essere eseguiti anche come attività pianificate. Per configurare un'attività pianificata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET Endpoint Antivirus sono attivate le seguenti attività:

- **Aggiornamento automatico periodico**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna di queste attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, consultare Pianificazione attività 23.

11.3 Aggiornamento a una nuova build

Per assicurare la massima protezione, è importante utilizzare la build più recente di ESET Endpoint Antivirus. Per verificare la disponibilità di una nuova versione, fare clic su **Aggiorna** dal menu principale a sinistra. Se è disponibile una nuova build, sulla parte inferiore della finestra verrà visualizzata una notifica. Fare clic su **Per saperne di più** per visualizzare una nuova finestra contenente il numero di versione della nuova build e il changelog.

Fare clic su **Scarica** per scaricare la build più recente. Fare clic su **Chiudi** per chiudere la finestra e scaricare l'aggiornamento in seguito.

Se si seleziona **Scarica**, il file verrà scaricato nella cartella Download o nella cartella predefinita impostata dal browser in uso. Al termine del download, avviare il file e attenersi alle istruzioni di installazione. Le informazioni sulla licenza verranno trasferite automaticamente alla nuova installazione.

Si consiglia di verificare periodicamente la disponibilità degli aggiornamenti, soprattutto quando si esegue l'installazione di ESET Endpoint Antivirus tramite CD/DVD.

11.4 Aggiornamenti sistema

La funzione degli aggiornamenti di sistema per Mac OS X rappresenta un componente importante pensato per garantire agli utenti protezione contro software dannoso. Per un livello di protezione massimo, si raccomanda di installare gli aggiornamenti non appena disponibili. ESET Endpoint Antivirus invierà all'utente una notifica relativa agli aggiornamenti mancanti in base al livello di importanza. È possibile regolare il livello di importanza di un aggiornamento per il quale vengono visualizzate le notifiche in **Configurazione** > **Inserisci preferenze applicazione** > **Avvisi e notifiche** > **Configurazione** utilizzando il menu a discesa **Visualizza condizioni** accanto a **Aggiornamenti sistema operativo**.

- **Mostra tutti gli aggiornamenti** - verrà visualizzata una notifica tutte le volte che verrà rilevata la mancanza di un aggiornamento di sistema
- **Mostra solo consigliati** - l'utente riceverà esclusivamente le notifiche relative agli aggiornamenti consigliati

Se non si desidera ricevere notifiche relative agli aggiornamenti mancanti, deselezionare la casella di controllo accanto a **Aggiornamenti sistema operativo**.

La finestra delle notifiche fornisce una panoramica degli aggiornamenti disponibili per il sistema operativo OS X e delle applicazioni aggiornate mediante lo strumento nativo di OS X chiamato "Aggiornamenti software". È possibile eseguire l'aggiornamento direttamente dalla finestra delle notifiche oppure dalla sezione **Home** di ESET Endpoint Antivirus facendo clic su **Installa aggiornamento mancante**.

La finestra delle notifiche contiene il nome, la versione, le dimensioni e le proprietà (flag) dell'applicazione, nonché informazioni aggiuntive sugli aggiornamenti disponibili. La colonna **Flag** contiene le seguenti informazioni:

- **[scelta consigliata]** - il produttore del sistema operativo consiglia di installare questo aggiornamento allo scopo di potenziare il livello di protezione e di stabilità del sistema
- **[riavvia]** - in seguito all'installazione, è necessario riavviare il computer
- **[arresta]** - in seguito all'installazione, è necessario spegnere e riaccendere il computer

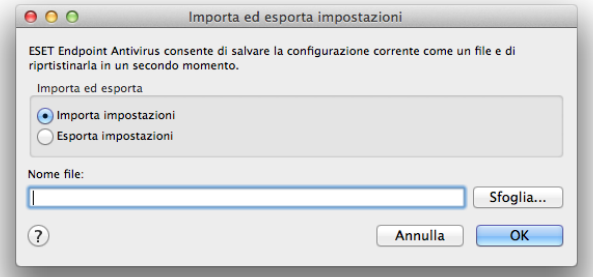
La finestra delle notifiche mostra gli aggiornamenti recuperati dallo strumento della riga di comando chiamato "aggiornamentosoftware". Gli aggiornamenti recuperati da questo strumento sono diversi da quelli visualizzati nell'applicazione "Aggiornamenti software". Se si desidera installare tutti gli aggiornamenti disponibili visualizzati nella finestra "Aggiornamenti di sistema mancanti", oltre a quelli non visualizzati nell'applicazione "Aggiornamenti software", è necessario utilizzare lo strumento della riga di comando "aggiornamentosoftware". Per ulteriori informazioni su questo strumento, leggere il manuale "aggiornamentosoftware" digitando `man softwareupdate` in una finestra del **Terminale**. L'utilizzo di questa opzione è consigliato esclusivamente agli utenti avanzati.

12. Varie

12.1 Importa ed esporta impostazioni

Per importare una configurazione esistente o esportare la propria configurazione di ESET Endpoint Antivirus, fare clic su **Configurazione** > **Importa ed esporta impostazioni**.

Le opzioni di importazione e di esportazione sono utili nel caso in cui si desideri effettuare il backup della configurazione corrente di ESET Endpoint Antivirus per utilizzi successivi. La funzione Esporta impostazioni è inoltre utile per quegli utenti che desiderano utilizzare la configurazione preferita di ESET Endpoint Antivirus su più di un sistema. È possibile importare facilmente un file di configurazione per trasferire le impostazioni desiderate.



12.1.1 Importa impostazioni

Per importare una configurazione, fare clic su **Configurazione** > **Importa ed esporta impostazioni** dal menu principale, quindi selezionare **Importa impostazioni**. Fare clic su **Sfoglia** per accedere al file di configurazione che si desidera importare.

12.1.2 Esporta impostazioni

Per esportare una configurazione, fare clic su **Configurazione** > **Importa ed esporta impostazioni** dal menu principale e selezionare **Esporta impostazioni**. Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.

12.2 Configurazione del server proxy

Per configurare le impostazioni del server proxy, fare clic su **Configurazione** > **Inserisci preferenze applicazione** > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per tutte le funzioni di ESET Endpoint Antivirus. I parametri definiti in questa sezione verranno utilizzati da tutti i moduli che richiedono una connessione a Internet. ESET Endpoint Antivirus supporta l'autenticazione Basic Access e NTLM (NT LAN Manager).

Per specificare le impostazioni del server proxy per questo livello, selezionare **Utilizza server proxy** e inserire l'indirizzo IP o URL del server proxy nel campo **Server proxy**. Nel campo **Porta**, specificare la porta sulla quale il server proxy accetta le connessioni (in base alle impostazioni predefinite, la porta 3128).

Se la comunicazione con il server proxy richiede l'autenticazione, inserire un **Nome utente** e una **Password** validi nei rispettivi campi.

12.3 Cache locale condivisa

Per attivare l'utilizzo della cache locale condivisa, fare clic su Configurazione > Inserisci preferenze applicazione > Cache locale condivisa e selezionare la casella di controllo accanto a Attiva memorizzazione nella cache tramite ESET Shared Local Cache. L'utilizzo di questa funzione potenzia le prestazioni negli ambienti virtuali eliminando i controlli duplicati nella rete. Ciò garantisce un controllo unico di ciascun file e l'archiviazione nella cache condivisa. Attivando questa opzione, le informazioni relative ai controlli di file e cartelle presenti nella rete dell'utente vengono salvate nella cache locale. Se si esegue un nuovo controllo, ESET Endpoint Antivirus ricercherà i file controllati nella cache. In caso di corrispondenza tra i file, questi verranno esclusi dal controllo.

Le impostazioni relative alla cache locale condivisa prevedono le seguenti opzioni:

- **Indirizzo server** - nome o indirizzo IP del computer in cui è collocata la cache
- **Porta** - numero della porta utilizzata per le comunicazioni (3537 per impostazione predefinita)
- **Password** - password della cache locale condivisa (facoltativo)

NOTA: per istruzioni più dettagliate sulle modalità di installazione e configurazione di ESET Shared Local Cache, consultare il manuale utente di ESET Shared Local Cache. (Disponibile solo in lingua inglese).